FRONTIERS OF PHYSICS

LECTURE NOTES
Volume 19 / Issue 5 / 51203 / 2024

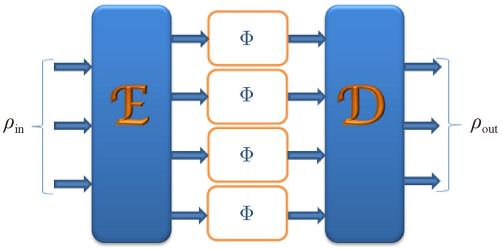
Lecture notes on quantum entanglement: From stabilizer states to stabilizer channels

Amir R. Arab[1,2]

1 Steklov Mathematical Institute of Russian Academy of Sciences, Gubkina Str., 8, Moscow 119991, Russia
2 Moscow Institute of Physics and Technology, 9 Institutskiy Per., Dolgoprudny, Moscow Region, 141701, Russia
E-mail: amir.arab@phystech.edu
Received January 15, 2024; accepted February 26, 2024

ABSTRACT

We study mathematical, physical and computational aspects of the stabilizer formalism arising in quantum information and quantum computation. The measurement process of Pauli observables with its algorithm is given. It is shown that to detect genuine entanglement we need a full set of stabilizer generators and the stabilizer witness is coarser than the GHZ (Greenberger–Horne–Zeilinger) witness. We discuss stabilizer codes and construct a stabilizer code from a given linear code. We also discuss quantum error correction, error recovery criteria and syndrome extraction. The symplectic structure of the stabilizer formalism is established and it is shown that any stabilizer code is unitarily equivalent to a trivial code. The structure of graph codes as stabilizer codes is identified by obtaining the respective stabilizer generators. The distance of embeddable stabilizer codes in lattices is obtained. We discuss the Knill–Gottesman theorem, tableau representation and frame representation. The runtime of simulating stabilizer gates is obtained by applying stabilizer matrices. Furthermore, an algorithm for updating global phases is given. Resolution of quantum channels into stabilizer channels is shown. We discuss capacity achieving codes to obtain the capacity of the quantum erasure channel. Finally, we discuss the shadow tomography problem and an algorithm for constructing classical shadow is given.



Keywords Pauli product, stabilizer state, measurement process, entanglement detection, stabilizer code, stabilizer circuit, quantum channel, tomography

Contents

Higher Education Press

https://doi.org/10.1007/s11467-024-1397-4

1 Introduction

The stabilizer formalism was originally introduced to describe quantum error-correcting codes [1], but now plays many different roles in quantum information and quantum computation. The key idea of this formalism is that quantum states can be represented by operators that stabilize them. A quantum system is fully described by a quantum state, which is viewed as a mathematical object. The description of quantum states is a complicated task, because we need exponentially many parameters in the number of qubits [2]. The stabilizer formalism is a powerful tool to describe a considerable class of entangled states.

One of the challenges facing quantum computation and other attempts to create specific highly entangled states is decoherence and controlling operational errors. A subclass of quantum codes, the stabilizer codes, has developed based on a group theoretical approach to meet this challenge [3]. A stabilizer quantum error-correcting code encodes logical qubits into physical qubits. In other words, a stabilizer code appends ancilla qubits to qubits that we want to protect. Stabilizer codes have found a wide range of applications, for instance, decoherence-free stabilizer codes are constructed for open quantum systems [4] and stabilizer codes are related to Lorentzian lattices and non-chiral CFTs [5].

An n-qubit stabilizer state is the simultaneous $+1$ eigenvector of n independent, commuting elements of the Pauli group. A graph state is a special type of multi-qubit state that can be represented by a graph. Stabilizer states and graph states have applications in quantum error correction and form a universal resource for measurement-based quantum computation [6]. The class of stabilizer states is rich enough to be considered useful in almost all applications of quantum networks. For example, the GHZ-state is seen in many quantum protocols [7]. Some of these applications include quantum secret sharing [8], conference key agreement [9], anonymous transfer [10] and clock synchronization [11].

A stabilizer circuit is a quantum circuit in which every gate is a controlled-NOT, Hadamard, phase, or 1-qubit measurement gate. Stabilizer circuits can be applied to create highly entangled states. They also perform the encoding and decoding steps for quantum error-correcting codes. They also play a central role in fault-tolerant circuits [12]. The stabilizer formalism enables us to encompass most of the paradoxes of quantum mechanics including dense quantum coding [13], the GHZ experiment [14] and quantum teleportation [15]. However, the Knill–Gottesman theorem allows such circuits to be simulated classically with an efficient runtime [16].

This paper is devoted to the description of the stabilizer formalism and its applications arising in quantum information and quantum computation. This paper is organized as follows. In Section 2, we provide basic definitions and lemmas on stabilizer states, binary representation and Clifford group. In Section 3, we study the measurement process of a Pauli observable by using the projective measurement and give the respective algorithm based on stabilizer generators. In Section 4, we introduce two fundamental concepts of "entanglement detection" and "entanglement witness". Then it is shown that the stabilizer witness is coarser than the GHZ witness by applying the GHZ basis and methods of operator theory. Furthermore, it is shown that to detect genuine entanglement by stabilizer witness we need a full set of stabilizer generators. In this way, we apply methods of standard linear algebra. In Section 5, we give basic definitions and important instances of stabilizer codes, then a stabilizer code is constructed from a given classical linear code. We discuss Pauli errors, error-correcting codes and the process of syndrome extraction. The symplectic structure of the stabilizer formalism is established and it is shown that any stabilizer code with k logical qubits is unitarily equivalent to a k-trivial stabilizer code. Two equivalent definitions of graph states are given. Graph codes associated with linear codes are characterized and it is shown that any graph code is a stabilizer code by identifying its stabilizer generators. The cleaning lemma based on independent logical operators is shown and the distance of an embeddable code in a lattice is obtained. Generalization of stabilizer codes and Clifford group is given. In Section 6, stabilizer gates are introduced and their simulating runtime is obtained by applying stabilizer matrices. The Knill–Gottesman theorem, tableau representation and frame representation are discussed. The runtime of resolution of a Pauli group element into production of a stabilizer state and a destabilizer state is obtained. The algorithm for updating global phases is given. In

Section 7, we discuss stabilizer channels and their types including Pauli reset channels and Clifford channels. Resolution of a quantum channel into a sum of stabilizer channels is given. The key concept of negativity is discussed. The capacity of the quantum erasure channel is obtained by a class of capacity achieving stabilizer codes. In Section 8, we discuss shadow tomography problem and the framework of classical shadow estimation is given as an algorithm. And finally, in Section 9 we present some research lines.

2 Pauli products

The *Pauli operators* on a two-level quantum system $H \simeq \mathbb{C}^2$ (qubit) are defined as follows:

$$\sigma_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\sigma_y = Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \ \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

where H is the Hilbert space on which the operators act. The *Pauli group* $\mathcal{P}$ is defined as the group generated by the Pauli operators up to the phase factors ± 1, $\pm\mathrm{i}$, i.e.,

$$\mathcal{P} = \langle \{\pm 1, \pm\mathrm{i}\} \times \{I, X, Y, Z\} \rangle.$$

For n qubits, the Pauli group is defined as

$$\mathcal{P}_n = \mathcal{P}^{\otimes n} = \big\{ \mathrm{i}^k \sigma_1 \otimes \sigma_2 \otimes ... \otimes \sigma_n : k \in \{0,1,2,3\}, \\ \sigma_j \in \{I, X, Y, Z\} \big\}.$$

Pauli operators on qubit j form a basis for the operator space on a single qubit. Products of operators of this sort, called *Pauli products*, span the space of operators on n qubits. If u is an operator on n qubits, its *base* is the set of qubits on which it acts nontrivially (X, Y, or Z). The *weight* $w(u)$ of u is the number of qubits in its base. For example

$$X_1 Z_1 Z_2 X_3 Z_5 = X_1 Z_1 \otimes Z_2 \otimes X_3 \otimes I_4 \otimes Z_5 \\ \otimes I_6 \otimes ... \otimes I_n,$$

has base $\{1,2,3,5\}$, so is of weight 4. Here, the index (of operators) indicates the Hilbert space (qubit) that the respective operator acts on.

2.1 Stabilizer states

A *stabilizer* S of n qubits is an Abelian subgroup of $\mathcal{P}_n$ that does not include $-I = -I^{\otimes n}$. Let $S = \langle g_1, g_2, ..., g_k \rangle$, where $g_j \in \mathcal{P}_n$ are commuting and independent (i.e., no one can be expressed as a product of other generators, up to a sign) generators. Every element of the Pauli group is either Hermitian operator or anti-Hermitian operator. Any Hermitian operator has order two, i.e., $g_j^2 = g_j g_j^\dagger = I$ where $g_j^\dagger$ is the adjoint operator, and any anti-Hermitian operator has order four, i.e., $(\mathrm{i}g_j)^4 = I$. Therefore, S cannot contain anti-Hermitian operators as otherwise $-I \in S$. It shows that $|S| = 2^k$. When $|S| = 2^n$, there is a state $|\psi\rangle$ that is the common eigenvector of elements of S and is called a *stabilizer state*. For example, the EPR (Einstein–Podolsky–Rosen) state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ is a stabilizer state, because it is a $+1$ eigenvector of the stabilizer subgroup $\langle X \otimes X, Z \otimes Z \rangle$. The *stabilized subspace* V_S is defined as follows

$$V_S = \{|\psi\rangle \in H^{\otimes n} : s|\psi\rangle = |\psi\rangle, \forall s \in S\}.$$

An n-qubit GHZ state is defined by $|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$. In fact, the GHZ state is a $+1$ eigenvector of the following Pauli products:

$$\mathfrak{g}_1 := X_1 X_2 ... X_n, \ \ \mathfrak{g}_k := Z_{k-1} Z_k \ (k = 2, ..., n).$$

In other words, $\mathfrak{g}_k |GHZ\rangle = |GHZ\rangle$ for $k = 1, ..., n$. Let $S = \langle \mathfrak{g}_1, \mathfrak{g}_2, ..., \mathfrak{g}_n \rangle$ be the stabilizer generated by $\mathfrak{g}_1, \mathfrak{g}_2, ..., \mathfrak{g}_n$. Then $|S| = 2^n$ and by letting $S = \{s_1, s_2, ..., s_{2^n}\}$, we have

$$|GHZ\rangle\langle GHZ| = 2^{-n} \sum_{k=1}^{2^n} s_k = 2^{-n} \prod_{k=1}^{n} (I + \mathfrak{g}_k). \qquad (1)$$

We will apply Eq. (1) in Section 4.

2.2 Binary representation

At each qubit we use the following encoding of the Pauli operators as pairs of bits:

$$b(I) = (0|0), \ b(X) = (1|0), \ b(Y) = (1|1), \ b(Z) = (0|1).$$

We can reconstruct the Pauli operators as follows:

$$\sigma_j = \mathrm{i}^{b_1(\sigma_j) b_2(\sigma_j)} X^{b_1(\sigma_j)} Z^{b_2(\sigma_j)}, \qquad (2)$$

where $b(\sigma_j) = (b_1(\sigma_j)|b_2(\sigma_j))$. By applying Eq. (2) it follows that

$$b(\sigma_j \sigma_k) = b(\sigma_j) + b(\sigma_k),$$

$$b(\sigma_j) J b^{\mathrm{t}}(\sigma_k) = \begin{cases} 0 & \text{if } [\sigma_j, \sigma_k] = 0, \\ 1 & \text{if } \{\sigma_j, \sigma_k\} = 0, \end{cases} \qquad (3)$$

where $J = \begin{pmatrix} \mathbf{0} & I \\ I & \mathbf{0} \end{pmatrix}$, $[A, B] = AB - BA$, $\{A, B\} = AB + BA$, "t" is transposition and computations are done modulo 2. The left side of Eq. (3) is the symplectic inner product of the binary vectors. For example, using this notation, the Pauli product $u = X_1 Z_2 Z_5$ acting on $(\mathbb{C}^2)^{\otimes 5}$ has the following encoding

$$b(u) = (10000|01001) \in \mathbb{F}_2^{10},$$

where $\mathbb{F}_2$ is the binary field.

Lemma 1. *For every $u, v, w \in \mathcal{P}_n$ with corresponding binary vectors $b(u), b(v), b(w) \in \mathbb{F}_2^{2n}$, in encoding $b : \mathcal{P}_n \to \mathbb{F}_2^{2n}$,*

i) $uv \sim w \iff b(u) + b(v) = b(w)$,

ii) $[u,v]=0 \Longleftrightarrow b(u)Jb^{\mathrm{t}}(v)=0$,
where $\sim$ *denotes equality up to a global phase.*

Proof. It is derived from the following representation:

$$u = \mathrm{i}^{\sum_{j=1}^{n}[b_1(u)]_j[b_2(u)]_j} \prod_{j=1}^{n} X_j^{[b_1(u)]_j} \prod_{j=1}^{n} Z_j^{[b_2(u)]_j},$$

where $b(u)=(b_1(u)|b_2(u))$. □

Remark 1. Property (i) shows that the encoding is a homomorphism of groups, and property (ii) shows that when two Pauli products commute. Throughout this paper, the phrase "up to a global phase" means that we can ignore global phases.

For a given set of Pauli products $u_1,u_2,...,u_r$, the $r\times 2n$ matrix

$$G=\begin{pmatrix} b(u_1)\\ b(u_2)\\ \vdots\\ b(u_r)\end{pmatrix}$$

is called the *parity-check matrix* corresponding to the Pauli products.

Corollary 1. *A set of Pauli products* $g_1,g_2,...,g_n$ *with parity-check matrix* G *are stabilizer generators of a stabilizer state if and only if the following conditions hold*

i) $GJG^{\mathrm{t}}=\mathbf{0}$,
ii) G *has full rank.*

Proof. It follows from Lemma 1. □

2.3 Clifford group

The *Clifford group on* n *qubits* is defined as follows $\mathcal{C}_n=\{u\in U(2^n): u\mathcal{P}_n u^\dagger=\mathcal{P}_n\}$, where $U(2^n)$ is the unitary group of degree 2^n. We take into account that the action of every $u\in\mathcal{C}_1$ is completely determined by the images of X and Z, moreover $uXu^\dagger$ and $uZu^\dagger$ must anti-commute. Then, X can go to any element of $\{\pm X,\pm Y,\pm Z\}$ (since σ is Hermitian if and only if $u\sigma u^\dagger$ is Hermitian) and Z can go to any element of $\{\pm X,\pm Y,\pm Z\}\setminus\{\pm uXu^\dagger\}$. Therefore, including the global phase $\mathcal{C}_1$ has $8\times 24=128$ elements. In general, $|\mathcal{C}_n|=8\prod_{i=1}^{n}2(4^i-1)4^i$ [17]. We note that qubit $|q\rangle=\cos(\frac{\theta}{2})|0\rangle+\mathrm{e}^{\mathrm{i}\varphi}\sin(\frac{\theta}{2})|1\rangle$ on the Bloch sphere can be written as $\boldsymbol{q}=(\sin\theta\cos\varphi,\sin\theta\sin\varphi,\cos\theta)$. Let $\boldsymbol{\sigma}=(\sigma_x,\sigma_y,\sigma_z)$ and define

$$\begin{aligned} M_q=\boldsymbol{q}\cdot\boldsymbol{\sigma}&=\sin\theta\cos\varphi\,\sigma_x+\sin\theta\sin\varphi\,\sigma_y+\cos\theta\,\sigma_z\\ &=\begin{pmatrix}\cos\theta & \mathrm{e}^{-\mathrm{i}\varphi}\sin\theta\\ \mathrm{e}^{\mathrm{i}\varphi}\sin\theta & -\cos\theta\end{pmatrix}.\end{aligned}$$

A qubit rotation by angle α about the arbitrary axis $\hat{n}$ is written as a *similarity transformation*, i.e., $M_{q'}=U_{\hat{n}}(\alpha)M_qU_{\hat{n}}(\alpha)^\dagger$, where $U_{\hat{n}}(\alpha)=\mathrm{e}^{-\mathrm{i}\frac{\alpha}{2}\hat{n}\cdot\boldsymbol{\sigma}}=\cos(\frac{\alpha}{2})I-\mathrm{i}\sin(\frac{\alpha}{2})(\hat{n}\cdot\boldsymbol{\sigma})$. We can think of $\mathcal{C}_1$ as rotations of the Bloch sphere that permute $\pm x,\pm y,\pm z$ directions.

3 Measurement process

In this section, we study the process of measuring a *Pauli observable*, i.e., Hermitian Pauli group element, O on a stabilizer state $|\psi\rangle$. We recall that the projective measurement described by O is based on the decomposition $O=\sum_k\lambda_kP_k$, where P_k is the projector onto the eigenvector of O with eigenvalue λ_k. Upon measuring, the probability of getting result λ_k is $p(k)=\langle\psi|P_k|\psi\rangle$. Given that outcome λ_k occured, the post-measurement state is $\frac{P_k|\psi\rangle}{\sqrt{p(k)}}$.

Lemma 2. *Adding an independent and commuting generator to the set of stabilizer generators cuts the stabilized subspace dimension in half.*

Proof. Given a generator g,

$$\left[\frac{1}{2}(I+g)\right]^2=\frac{1}{4}(I+2g+g^2)=\frac{1}{4}(I+2g+I)=\frac{1}{2}(I+g),$$

thus $P_g=\frac{1}{2}(I+g)$ is a projector. We note that $P_g|\psi\rangle=|\psi\rangle$ if and only if $g|\psi\rangle=|\psi\rangle$, and $P_g|\psi\rangle=0$ if and only if $g|\psi\rangle=-|\psi\rangle$, thus P_g is the projector onto V_S, where $S=\langle g\rangle$ and

$$\dim V_S=\mathrm{tr}P_g=\mathrm{tr}\left[\frac{1}{2}(I+g)\right]=\mathrm{tr}\left[\frac{I}{2}\right]=2^{n-1}.$$

By adding an independent and commuting generator h to S, we have

$$P_g|\psi\rangle=|\psi\rangle, P_h|\psi\rangle=|\psi\rangle\Longleftrightarrow P_gP_h|\psi\rangle=|\psi\rangle,$$

and it means that the subspace stabilized by both g and h is of dimension $\mathrm{tr}[P_gP_h]=2^{n-2}$. By induction on the number of generators of S, the proof is completed. □

Let $S=\langle g_1,g_2,...,g_n\rangle$ be a set of stabilizer generators for $|\psi\rangle$. There are two cases:

Case I. For every j, O commutes with g_j. From Lemma 1, it follows that O cannot be independent of the generators in S. Hence, $O=(-1)^kg_1^{k_1}g_2^{k_2}...g_n^{k_n}$, where $k,k_j\in\{0,1\}$. Therefore,

$$O|\psi\rangle=(-1)^kg_1^{k_1}g_2^{k_2}...g_n^{k_n}|\psi\rangle=(-1)^k|\psi\rangle,$$

measurement O gives result $(-1)^k$ with probability

$$\begin{aligned} p((-1)^k)&=\langle\psi|\frac{1}{2}(I+(-1)^kO)|\psi\rangle\\ &=\frac{1}{2}\langle\psi|\psi\rangle+\frac{(-1)^k(-1)^k}{2}\langle\psi|\psi\rangle=1,\end{aligned}$$

and the post-measurement state is $\frac{1}{2}(I+(-1)^kO)|\psi\rangle=|\psi\rangle$.

Case II. There is a generator g in S, such that O anti-commutes with g. For a given generator g_j, O either commutes with or anti-commutes with g_j. In the first case, we do not change g_j, but in the second case we construct a new set of generators as follows. We note that $Ogg_j=-gOg_j=gg_jO$, then gg_j is a generator that

commutes with O. g_j is replaced by gg_j and it is also denoted by g_j. The action of g_j on the (un-normalized) post-measurement state is

$$g_j\left(\frac{1}{2}\right)[I+(-1)^k O]|\psi\rangle = \frac{1}{2}[I+(-1)^k O]g_j|\psi\rangle = \frac{1}{2}[I+(-1)^k O]|\psi\rangle,$$

where $(-1)^k$ is the measurement outcome. Now, we only need one more independent stabilizer generator (instead of g) to characterize the post-measurement state completely. The key idea is that an n–qubit stabilizer state is uniquely determined by n stabilizing operators. O is the generator that is needed because, firstly, O anti-commutes with g, so it is independent of all the generators. Furthermore, $(-1)^k O$ stabilizes the post-measurement state as follows:

$$(-1)^k O\left(\frac{1}{2}\right)[I+(-1)^k O]|\psi\rangle = \frac{1}{2}[(-1)^k O+I]|\psi\rangle.$$

This argument shows that by obtaining the measurement outcome $(-1)^k$, we reach stabilizer generators for the post-measurement state to be $g_j \neq g$ and $(-1)^k O$. The measurement outcomes are ± 1 with equal probability, because

$$\mathbb{E}(O) = \langle\psi|O|\psi\rangle = \langle\psi|Og|\psi\rangle = \langle\psi| - gO|\psi\rangle = -\langle\psi|O|\psi\rangle,$$

or $\langle\psi|O|\psi\rangle = 0$.

From this discussion, it results the following algorithm to measure a Pauli observable O in a stabilizer state $|\psi\rangle$:

Algorithm 1. (Measurement process)

1) Find a set of stabilizer generators for $|\psi\rangle$ such that at most one generator anti-commutes with O.

2) If all the stabilizer generators commute with O, then the outcome will be certain and the post-measurement state will be $|\psi\rangle$.

3) If one generator, say g, anti-commutes with O, then outcome will be random and by replacing g with $\pm O$ we reach a new set of generators that stabilize the post-measurement state.

In the following section, we present the method of entanglement witnesses as the most common entanglement detection tool.

4 Entanglement detection

Entangled state $|\psi\rangle$ describes a system made of two separable parts which cannot be written as a tensor product of states $|\psi_1\rangle$ and $|\psi_2\rangle$ describing separately each of the subsystems, i.e., $|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$. A pure state is called *biseparable*, if it can be written as a tensor product of two multi-partite states $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, we take into account that each of $|\psi_1\rangle$ and $|\psi_2\rangle$ can be an entangled state. A mixed state is biseparable, if it can be written as a convex combination of biseparable pure states, i.e., $\rho = \sum_i p_i |\psi_i\rangle_1\langle\psi_i| \otimes |\phi_i\rangle_2\langle\phi_i|$ with $p_i \geq 0$ and $\sum_i p_i = 1$, where $|\psi_i\rangle$'s and $|\phi_i\rangle$'s are biseparable pure states. A state that is not biseparable is called *genuine multipartite entangled.*

Theorem 1. ([18]) *A density operator ρ on $\mathcal{H}_1 \otimes \mathcal{H}_2$, where $\mathcal{H}_i$'s are Hilbert spaces, is entangled if and only if there exists a Hermitian operator w such that* $\mathrm{tr}[w\rho] < 0$, *and for all separable states ρ_{sep},* $\mathrm{tr}[w\rho_{\mathrm{sep}}] \geq 0$. *$w$ is called entanglement witness.*

Let $|\psi\rangle$ be a pure state, B be a fixed bipartite splitting, and consider product states $|\phi\rangle \in B$. By choosing an orthonormal product basis $|ij\rangle$ for partition B, we can write

$$|\psi\rangle = \sum_{i,j} \gamma_{ij}|ij\rangle, \quad |\phi\rangle = |\alpha\beta\rangle = \sum_{i,j} \alpha_i\beta_j|ij\rangle.$$

Let $\gamma = (\gamma_{ij})$ be the coefficient matrix, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ be the normalized coefficient vectors. Thus

$$\max_{|\phi\rangle\in B} |\langle\phi|\psi\rangle| = \max_{\alpha_i,\beta_j} |\sum_{i,j}(\alpha_i^*\gamma_{ij}\beta_j^*)| = \max_{\boldsymbol{\alpha},\boldsymbol{\beta}} |\langle\boldsymbol{\alpha}|\gamma|\boldsymbol{\beta}^*\rangle| = \max_k \{\lambda_k(\gamma)\},$$

where $\lambda_k(\gamma)$ denotes the singular values of γ. In other words, $\lambda_k(\gamma)$ are the Schmidt coefficients of $|\psi\rangle$ with respect to bipartite splitting B. Let m be the square of the maximal Schmidt coefficient over all possible bipartite partitions of $|\psi\rangle$. Therefore, $\mathcal{W}_\psi = mI - |\psi\rangle\langle\psi|$ is a witness operator that detects genuine multipartite entanglement of $|\psi\rangle$. We can summarize this discussion in the following lemma.

Lemma 3. *A witness operator that detects genuine multipartite entanglement of a pure state $|\psi\rangle$ is given by $\mathcal{W}_\psi = mI - |\psi\rangle\langle\psi|$, where I is the identity operator and $m = \max_{|\phi\rangle\in B} |\langle\phi|\psi\rangle|^2$, where B denotes the set of biseparable states.*

Corollary 2. *For $|\psi\rangle = |GHZ\rangle$, $\mathcal{W}_{GHZ} = \frac{1}{2}I - |GHZ\rangle\langle GHZ|$.*

The witness $\mathcal{W}_{\mathrm{GHZ}}$ detects genuine n-qubit entanglement around the GHZ state, which has been applied in an experiment [19]. By applying Eq. (1), it turns out that $\mathcal{W}_{\mathrm{GHZ}}$ is a stabilizer witness, i.e., constructed by stabilizer generators, and can be measured locally, i.e., can be written as a sum of Pauli products. But the number of measurement settings increases exponentially with the number of qubits [20], which is not appropriate.

The *GHZ state basis* $\mathcal{B}$ is defined as the set of the following states

$$\frac{1}{\sqrt{2}}\left(|x^1...x^n\rangle \pm |\tilde{x}^1...\tilde{x}^n\rangle\right),$$

where $x^i \in \{0,1\}$ and $\tilde{x}^i = 1 - x^i$ for $i = 1,...,n$. $\mathcal{B}$ is an orthogonal basis and $|\mathcal{B}| = 2^n$. We represent elements of $\mathcal{B}$ as $|B\rangle$.

For a given entanglement witness $\mathcal{W}$, let $D_{\mathcal{W}}$ be the

set of states which are detected by $\mathcal{W}$, i.e.,

$$D_{\mathcal{W}} := \{\rho \geq 0 : \mathrm{tr}[\mathcal{W}\rho] < 0\}.$$

For two given entanglement witnesses $\mathcal{W}_1$ and $\mathcal{W}_2$, we say that $\mathcal{W}_1$ is *finer* (*coarser*) than $\mathcal{W}_2$, if $D_{\mathcal{W}_2} \subset D_{\mathcal{W}_1}$ ($D_{\mathcal{W}_1} \subset D_{\mathcal{W}_2}$).

Theorem 2. *There is a stabilizer witness consisting of all the generators which is coarser than* $\mathcal{W}_{\mathrm{GHZ}}$.

Proof. It is shown that $\mathcal{W}_{\mathrm{stab}} = \frac{n-1}{2} I - \frac{1}{2}\sum_{k=1}^{n} \mathfrak{g}_k$ is the desired witness. We note that $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$, $Z|0\rangle = |0\rangle$ and $Z|1\rangle = -|1\rangle$. Let

$$T = (n-2)I - \sum_{k=1}^{n} \mathfrak{g}_k + 2|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|.$$

Given a basis element $|B\rangle \neq |\mathrm{GHZ}\rangle$, there exists a stabilizer generator $\mathfrak{g}_k$ such that $\mathfrak{g}_k|B\rangle = -|B\rangle$, because case 1: if $|B\rangle = \frac{|00\ldots0\rangle - |11\ldots1\rangle}{\sqrt{2}}$, then $\mathfrak{g}_1|B\rangle = -|B\rangle$, and case 2: if all of x^i's in $|B\rangle = \frac{1}{\sqrt{2}}\big(|x^1\ldots x^n\rangle \pm |\tilde{x}^1\ldots\tilde{x}^n\rangle\big)$ are not equal, let j be the first index for which $x^i \neq x^{i+1}$, then $\mathfrak{g}_{j+1}|B\rangle = -|B\rangle$. It follows that $T|B\rangle = \lambda_B|B\rangle$, where $\lambda_B \geq 0$. Furthermore, $T|\mathrm{GHZ}\rangle = 0$. It shows that all of the 2^n eigenvalues of T are nonnegative, thus $T \geq 0$. Hence, $\mathcal{W}_{\mathrm{stab}} \geq \mathcal{W}_{\mathrm{GHZ}}$ and then $\mathrm{tr}[\mathcal{W}_{\mathrm{stab}}\rho] \geq \mathrm{tr}[\mathcal{W}_{\mathrm{GHZ}}\rho]$ for every state ρ. It means that $D_{\mathcal{W}_{\mathrm{stab}}} \subset D_{\mathcal{W}_{\mathrm{GHZ}}}$. □

Theorem 2 shows that $\mathcal{W}_{\mathrm{stab}}$ detects only states with genuine n-qubit entanglement. In fact, $\mathcal{W}_{\mathrm{stab}}$ uses only two measurement settings: 1) $\{X_1, \ldots, X_n\}$ to measure $\mathbb{E}(\mathfrak{g}_1)$, and 2) $\{Z_1, \ldots, Z_n\}$ to measure $\mathbb{E}(\mathfrak{g}_2)$,..., $\mathbb{E}(\mathfrak{g}_n)$. This is the advantage of using $\mathcal{W}_{\mathrm{stab}}$.

Theorem 3. *In Theorem 2, we need a full set of generators to detect genuine entanglement. In other words, with less than n generators, we cannot detect genuine n-qubit entanglement.*

Proof. We remove one of the stabilizer generators, say $\mathfrak{g}_n$. We claim that there is a Pauli product $u \in \mathcal{P}_n$ such that u commutes with $\mathfrak{g}_i$ for $i = 1, \ldots, n-1$, and anticommutes with $\mathfrak{g}_n$. Since the parity check matrix G has full rank, then the system of equations

$$G_x = (0\ 0\ \ldots\ 0\ 1)^{\mathrm{t}}$$

has a solution $\boldsymbol{b} = \begin{pmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{pmatrix}$, where $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ are $n \times 1$ binary columns. Let $U = (\boldsymbol{b}_2^{\mathrm{t}} \quad \boldsymbol{b}_1^{\mathrm{t}})$, then for rows G_i of G, we have

$$G_i J U^{\mathrm{t}} = 0 \quad (i = 1, \ldots, n-1), \quad G_n J U^{\mathrm{t}} = 1.$$

Let u be the Pauli product corresponding to U, then according to Lemma 1, it turns out that $[u, \mathfrak{g}_i] = 0$ for $i = 1, \ldots, n-1$, and $u\mathfrak{g}_n \neq \mathfrak{g}_n u$. Let $\hat{\mathcal{W}}$ be the witness which is obtained from $\mathcal{W}_{\mathrm{stab}}$ by removing $\mathfrak{g}_n$. Since $u\mathfrak{g}_i = \mathfrak{g}_i u$ $(i = 1, \ldots, n-1)$, then the expectation values of $\hat{\mathcal{W}}$ in $|\mathrm{GHZ}\rangle$ and $|g'\rangle := u|\mathrm{GHZ}\rangle$ are equal and it means that there are at least two elements of the basis $\mathcal{B}$ which give the minimum. We note that $\langle\mathrm{GHZ}|\mathcal{W}_{\mathrm{stab}}|\mathrm{GHZ}\rangle = -\frac{1}{2}$, and for any basis element $|B\rangle \neq |\mathrm{GHZ}\rangle$, $\sum_{k=1}^{n}\langle B|\mathfrak{g}_k|B\rangle < n$, thus $\langle B|\mathcal{W}_{\mathrm{stab}}|B\rangle > -\frac{1}{2}$. Therefore, $\mathcal{W}_{\mathrm{stab}}$ takes the minimal value only for $|\mathrm{GHZ}\rangle$. There is a superposition of $|\mathrm{GHZ}\rangle$ and $|g'\rangle$ which is biseparable. It follows that the witness $\hat{\mathcal{W}}$ takes the minimal value in the biseparable state and then it is not applicable to detect genuine n-qubit entanglement. □

In the next section, we study stabilizer codes as a strong tool to correct errors in multiple qubit systems.

5 Stabilizer codes

In classical coding theory, our goal is to encode k classical bits (as k-bit strings) into binary codewords that are n-bit strings, say $v_k \mapsto v_n$. This is a *linear code*, if there exists an $k \times n$ full-rank matrix G_c such that $v_n = v_k G_c$. The matrix G_c is called the *generator matrix* of the code. The code is a k-dimensional subspace of $\mathbb{F}_2^n$ and is denoted by $\mathfrak{C} \in [n, k]$. The *distance* of $\mathfrak{C}$ is defined as $d := \min\{|\boldsymbol{c}| : \boldsymbol{c} \in \mathfrak{C}\}$, where $|\boldsymbol{c}| = |\{c_i : c_i = 1\}|$ with $\boldsymbol{c} = (c_1, \ldots, c_n)$. Here, it is denoted by $\mathfrak{C} \in [n, k, d]$. The *dual* of $\mathfrak{C}$ is a linear code defined as $\mathfrak{C}^{\perp} := \{\boldsymbol{x} \in \mathbb{F}_2^n : \langle \boldsymbol{x}, \boldsymbol{c}\rangle = 0, \forall \boldsymbol{c} \in \mathfrak{C}\}$, where $\langle ., . \rangle$ is the standard inner product. The *parity check matrix* of $\mathfrak{C}$ is the generator matrix of $\mathfrak{C}^{\perp}$ and is denoted by P_c.

Quantum stabilizer codes are quantum analogs of binary linear codes. Given an Abelian subgroup S of $\mathcal{P}_n$ which does not contain $-I$, the *(quantum) stabilizer code* corresponding to S is defined as $Q := V_S$. When S is generated by $n-k$ generators, the subspace Q has dimension 2^k (Lemma 2), it encodes k logical qubits to n physical qubits and it is denoted by $Q \in [[n, k]]$. The *distance* of the code is defined as $d := \min_{u \in N(S)\setminus S} w(u)$, where $N(S) = \{u \in \mathcal{P}_n : uSu^{\dagger} = S\}$ is the normalizer of S. The elements of $N(S) \setminus S$ are called nontrivial *logical operators* and trivial logical operators are elements of S. We denote the set of all logical operators by $\mathcal{L}$. Here, the code is denoted by $Q \in [[n, k, d]]$. For example, the 7-qubit code (Steane code) is a $[[7, 1, 3]]$ code with the following stabilizer

$$S = \big\langle Z_1Z_2Z_3Z_4, Z_1Z_2Z_5Z_6, Z_1Z_3Z_5Z_7, X_1X_2X_3X_4, X_1X_2X_5X_6, X_1X_3X_5X_7\big\rangle.$$

This code encodes 1 qubit to 7 qubits and its codewords are

$$\begin{aligned} |0\rangle_L = \frac{1}{\sqrt{8}}\big(&|0000000\rangle + |1010101\rangle + |0110011\rangle \\ &+ |1100110\rangle + |0001111\rangle + |1011010\rangle \\ &+ |0111100\rangle + |1101001\rangle\big), \\ |1\rangle_L = X_1X_2X_3X_4X_5X_6X_7|0\rangle_L. \end{aligned}$$

The Steane code belongs to the family of CSS (Calderbank–Shor–Steane) codes. A *CSS code* Q is a stabilizer

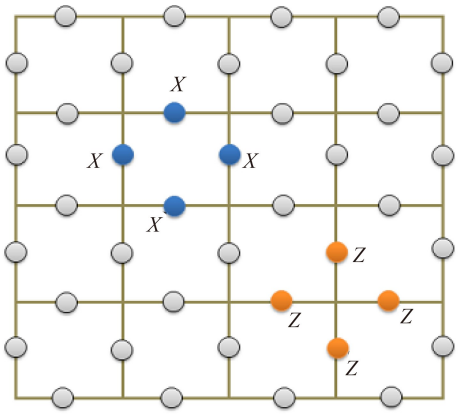


Fig. 1 Toric code.

code whose stabilizer S splits into two sets S_X and S_Z satisfying: 1) $S_X, S_Z \subset \mathcal{P}_n$ and S is the minimal group generated by S_X and S_Z. 2) If $u = \prod_{i=1}^n v_i \in S_X$, then $v_i \in \{I, X\}$. 3) If $u = \prod_{i=1}^n v_i \in S_Z$, then $v_i \in \{I, Z\}$. Let C_X and C_Z be the subgroups of $\mathbb{F}_2^{2n}$ corresponding to S_X and S_Z in Lemma 1, respectively. Hence, up to a global phase, we have the following bijection:

$$u_x = \prod_{i=1}^{n} v_i \in S_X \Longleftrightarrow \boldsymbol{c}_x = (c_1, ..., c_n) \in C_X,$$

where $c_i = 1(0)$ if and only if $v_i = X(I)$, and similarly for S_Z and C_Z. It follows that $\langle c_x, c_z \rangle = 0$, thus $C_Z \subseteq C_X^{\perp}$ and $C_X \subseteq C_Z^{\perp}$. In this example, the distance of the stabilizer code is defined as $d = \min_{\boldsymbol{c} \in C_X^{\perp} \setminus C_Z, C_Z^{\perp} \setminus C_X} |\boldsymbol{c}|$.

The toric code is an instance of CSS codes. Let Λ be a two-dimensional lattice, i.e., a set of vertices $\mathcal{V}$, edges $\mathfrak{E}$ and faces $\mathcal{F}$ glued together in a certain way. The *toric code* in two dimensions is defined on a lattice Λ by placing one qubit on every edge, and associating X- and Z-type generators with vertices and faces of Λ as follows:

$$\forall v \in \mathcal{V},\ X(v) := \prod_{e \in v} X(e), \quad \forall f \in \mathcal{F},\ Z(f) := \prod_{e \in f} Z(e),$$

where $X(e)$ and $Z(e)$ denote Pauli X and Z operators, respectively, acting on qubit placed on the edge e (see Fig. 1).

The Gottesman–Kitaev–Preskil (GKP) code is another instance of stabilizer codes. The GKP code is an n-mode quantum lattice code with $2n$ stabilizers, i.e., constructed using a non-degenerate lattice. This family of codes is quite important in fault-tolerant quantum computation. The GKP code is an important type of bosonic quantum error-correcting codes, which encodes a qubit in an oscillator [47].

A natural question gives rise: Given a linear code, how can we construct a stabilizer code? Let $\mathfrak{C}$ be an $[n, k]$ linear code with generator G_c. Let $A_1, ..., A_k$ be the rows of G_c. We extend the set of rows to a basis for $\mathbb{F}_2^n$ denoted by $\{A_1, ..., A_k, A_{k+1}, ..., A_n\}$. Let A be an $n \times n$ matrix with rows $A_1, ..., A_n$ and B be the inverse of A. Denote the columns of B by $B_1, ..., B_n$. By applying this notation $\boldsymbol{X}^{\boldsymbol{a}} := \prod_{i=1}^n X_i^{a_i}$ and $\boldsymbol{Z}^{\boldsymbol{a}} := \prod_{i=1}^n Z_i^{a_i}$, where $\boldsymbol{a} = (a_1, ..., a_n) \in \mathbb{F}_2^n$, we define the following $2n - k - 2$ generators on $2n - k - 1$ qubits:

$$\begin{aligned} g_i &= \boldsymbol{Z}^{A_i} \quad 1 \le i \le k, \\ g_{k+i} &= \boldsymbol{Z}^{A_{k+i}} Z_{n+i} \quad 1 \le i \le n-k-1, \\ g_{n-1+i} &= \boldsymbol{X}^{B_{k+i}} X_{n+i} \quad 1 \le i \le n-k-1. \end{aligned}$$

1) g_i's are independent. It follows from the linear independence of A_i's, the linear independence of B_i's, and the fact that the binary representation of X-type operators is linear independent of the binary representation of Z-type operators.

2) g_i's mutually commute. It is clear for the first $n-1$ generators and for the last $n-k-1$ generators. Between them, the commutation follows from the following identity

$$\boldsymbol{X}^{A_i} \boldsymbol{Z}^{B_j} = (-1)^{\langle A_i, B_j \rangle} \boldsymbol{Z}^{B_j} \boldsymbol{X}^{A_i},$$

and the fact that $\langle A_i, B_j \rangle = 0$ for $i \neq j$, and for $i = j$ the presence of X_{n+i} and Z_{n+i} guarantees commutation. Hence, $S = \langle g_1, ..., g_{2n-k-2} \rangle$ defines a $[[2n-k-1, 1]]$ stabilizer code.

5.1 Quantum error correction

Classical computers use repetition codes, i.e., each bit is encoded in many electrons, and after each time step the error correction is done, i.e., it is turned back to the value held by the majority of the electrons. The simplest example is the following repetition code: $0 \mapsto 000, 1 \mapsto 111$. It will correct the state 101 to the majority value 111. Because of the No–Cloning theorem, quantum computers cannot use a quantum repetition code as follows: $|\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$. The No–Cloning theorem says that there is no quantum operation that takes any state $|\psi\rangle$ to $|\psi\rangle \otimes |\psi\rangle$ [21].

Quantum error correction comes from meeting error correction in classical information theory and principles of quantum mechanics [23]. It is concerned with the main problem of communication in the presence of noise. Consider a single qubit in a pure state which interacts with its environment. Without loss of generality, we may assume that the initial state of the environment is pure, say $|0\rangle_E$. The evolution of the qubit and its environment is described by a unitary operator $\boldsymbol{U}$ as follows:

$$\begin{aligned} \boldsymbol{U}:\ & |0\rangle \otimes |0\rangle_E \mapsto |0\rangle \otimes |\phi_{00}\rangle_E + |1\rangle \otimes |\phi_{01}\rangle_E, \\ & |1\rangle \otimes |0\rangle_E \mapsto |0\rangle \otimes |\phi_{10}\rangle_E + |1\rangle \otimes |\phi_{11}\rangle_E, \end{aligned}$$

where $|\phi_{ij}\rangle_E$ are states of the environment. For an arbitrary state $|\psi\rangle = a|0\rangle + b|1\rangle$, we have

$$
\begin{aligned}
\boldsymbol{U}:\ & (a|0\rangle + b|1\rangle) \otimes |0\rangle_E \mapsto a(|0\rangle \otimes |\phi_{00}\rangle_E \\
& + |1\rangle \otimes |\phi_{01}\rangle_E) + b(|0\rangle \otimes |\phi_{10}\rangle_E + |1\rangle \otimes |\phi_{11}\rangle_E) \\
= & (a|0\rangle + b|1\rangle) \otimes \frac{1}{2}(|\phi_{00}\rangle_E + |\phi_{11}\rangle_E) \\
& + (a|0\rangle - b|1\rangle) \otimes \frac{1}{2}(|\phi_{00}\rangle_E - |\phi_{11}\rangle_E) \\
& + (a|1\rangle + b|0\rangle) \otimes \frac{1}{2}(|\phi_{01}\rangle_E + |\phi_{10}\rangle_E) \\
& + (a|1\rangle - b|0\rangle) \otimes \frac{1}{2}(|\phi_{01}\rangle_E - |\phi_{10}\rangle_E) \\
= & I|\psi\rangle \otimes |\phi_I\rangle_E + X|\psi\rangle \otimes |\phi_X\rangle_E \\
& + Y|\psi\rangle \otimes |\phi_Y\rangle_E + Z|\psi\rangle \otimes |\phi_Z\rangle_E.
\end{aligned}
$$

The interpretation of this expanding is that one of the following situations occurs to the qubit: trivial (I), bit flip (X), phase flip (Z), or both ($Y = iXZ$) (in practice, this classification makes sense when four states $|\phi_I\rangle_E, |\phi_X\rangle_E, |\phi_Y\rangle_E$ and $|\phi_Z\rangle_E$ of the environment are mutually orthogonal).

In general, for n qubits, the action of an arbitrary unitary operator can be described as follows:

$$
|\psi\rangle \otimes |0\rangle_E \mapsto \sum_u u|\psi\rangle \otimes |\phi_u\rangle_E,
$$

where u ranges over Pauli products and $|\phi_u\rangle_E$ are the corresponding states of the environment. We aim to identify a subset $\mathcal{E} \subset \mathcal{P}_n$ of correctable errors, i.e., the errors that we wish to be able to correct.

5.1.1 Error-correcting codes

A *quantum error-correcting code* is a mapping from the Hilbert space of dimension 2^k corresponding to k logical (encoded) qubits into the Hilbert space of dimension 2^n corresponding to n physical qubits, where $n > k$. The image of this mapping is called the *code subspace*. Our goal is to protect k encoded qubits from error. In this way, $n-k$ qubits are added as redundant qubits. Let $\{|\psi_i\rangle\}$ be an orthonormal basis for the code subspace, $|\psi_i\rangle$'s are called *codewords*. Now the quantum error correction criteria [22], i.e., a necessary and sufficient condition in terms of the codewords to preserve the code subspace, is proved.

Theorem 4. *Let $\mathcal{E} = \{E_a\}$ be a linear space of errors acting on the subspace code Q. Then recovery is possible if and only if*

$$
\langle\psi|E_b^\dagger E_a|\phi\rangle = 0, \tag{4}
$$

$$
\langle\psi|E_b^\dagger E_a|\psi\rangle = \langle\phi|E_b^\dagger E_a|\phi\rangle, \tag{5}
$$

$\forall a, b$ and $\forall |\psi\rangle \neq |\phi\rangle \in Q$.

Proof. Suppose that recovery is possible and let $\mathcal{R}$ be the unitary operator describing the whole recovery operation, then

$$
\mathcal{R}|\eta_a\rangle E_a|\phi\rangle = |\eta'_a\rangle|\phi\rangle, \ \ \mathcal{R}|\eta_b\rangle E_b|\psi\rangle = |\eta'_b\rangle|\psi\rangle,
$$

where $|\eta\rangle$'s are states of the ancilla (it is employed to implement the recovery operation) and the environment. Therefore,

$$
\langle\psi|E_b^\dagger\langle\eta_b|\mathcal{R}^\dagger\mathcal{R}|\eta_a\rangle E_a|\phi\rangle = \langle\eta'_b|\eta'_a\rangle\langle\psi|\phi\rangle.
$$

Since the recovery operation must work particularly when $|\eta_a\rangle = |\eta_b\rangle$, then $\langle\psi|E_b^\dagger E_a|\phi\rangle = 0$ and Eq. (4) is proven. To prove Eq. (5), we can write as follows:

$$
\begin{aligned}
& \mathcal{R}|\eta\rangle E_i|\psi\rangle = |\eta'_i\rangle|\psi\rangle, \ \ (i = a, b) \\
& \Rightarrow \langle\psi|E_b^\dagger\langle\eta|\mathcal{R}^\dagger\mathcal{R}|\eta\rangle E_a|\psi\rangle = \langle\eta'_b|\eta'_a\rangle \\
& \Rightarrow \langle\psi|E_b^\dagger E_a|\psi\rangle = \langle\eta'_b|\eta'_a\rangle.
\end{aligned}
$$

Similarly, by starting from $|\phi\rangle$, the same result is obtained and then Eq. (5) is proved. Analog of Eq. (5) is not possible in classical coding theory [42].

Suppose that Eqs. (4) and (5) or equivalently $\langle\psi_j|E_b^\dagger E_a|\psi_i\rangle = C_{ba}\delta_{ij}$ holds. It is clear that $C = [C_{ba}]$ is a Hermitian matrix. The action of an error on a basis state $|\psi_i\rangle$ and the environment is $|\psi_i\rangle \otimes |0\rangle_E \mapsto \sum_\alpha F_\alpha|\psi_i\rangle \otimes |\alpha\rangle_E$, where $|\alpha\rangle_E$'s are elements of an orthonormal basis for the environment, and F_α's are linear combinations of the Pauli products E_a's, satisfying the normalization condition

$$
\sum_\alpha F_\alpha^\dagger F_\alpha = I. \tag{6}
$$

It follows that $\langle\psi_j|F_\beta^\dagger F_\alpha|\psi_i\rangle = C_{\beta\alpha}\delta_{ij}$. The error can be reversed if there exist operators R_μ's such that $\sum_\mu R_\mu^\dagger R_\mu = I$ (normalization) and

$$
\sum_{\alpha,\mu} R_\mu F_\alpha|\psi_i\rangle \otimes |\alpha\rangle_E \otimes |\mu\rangle_A = |\psi_i\rangle \otimes |\vartheta\rangle_{EA},
$$

where $\{|\mu\rangle_A\}$ is an orthonormal basis for the Hilbert space of the ancilla and the state $|\vartheta\rangle_{EA}$ of environment and ancilla does not depend on i. The basis for the environment $\{|\alpha\rangle_E\}$ can be chosen such that the matrix C is diagonalized

$$
\langle\psi_j|F_\beta^\dagger F_\alpha|\psi_i\rangle = C_\alpha\delta_{\alpha\beta}\delta_{ij}, \tag{7}
$$

where $\sum_\alpha C_\alpha = 1$ follows from Eq. (6). For each μ with $C_\mu \neq 0$, let $R_\mu = \frac{1}{\sqrt{C_\mu}}\sum_i |\psi_i\rangle\langle\psi_i|F_\mu^\dagger$, therefore

$$
\begin{aligned}
& \sum_{\alpha,\mu} R_\mu F_\alpha|\psi_i\rangle \otimes |\alpha\rangle_E \otimes |\mu\rangle_A \\
& \quad = |\psi_i\rangle \otimes \big(\sum_\mu \sqrt{C_\mu}|\mu\rangle_E \otimes |\mu\rangle_A\big).
\end{aligned} \tag{8}
$$

Equation (8) shows that the R_μ's do indeed reverse the error. It remains to check the normalization condition. Let

$$R=\sum_{\mu}R_{\mu}^{\dagger}R_{\mu}=\sum_{\mu}\frac{1}{C_{\mu}}\sum_{i}F_{\mu}|\psi_i\rangle\langle\psi_i|F_{\mu}^{\dagger}.$$

By applying Eq. (7) it follows that

$$\begin{aligned}R^2&=(\sum_{\mu}\frac{1}{C_{\mu}}\sum_{i}F_{\mu}|\psi_i\rangle\langle\psi_i|F_{\mu}^{\dagger})(\sum_{\gamma}\frac{1}{C_{\gamma}}\sum_{j}F_{\gamma}|\psi_j\rangle\langle\psi_j|F_{\gamma}^{\dagger})\\&=\sum_{\mu}\frac{1}{C_{\mu}}\sum_{i}F_{\mu}|\psi_i\rangle\sum_{\gamma}\frac{1}{C_{\gamma}}\sum_{j}C_{\gamma}\delta_{\mu\gamma}\delta_{ij}\langle\psi_j|F_{\gamma}^{\dagger}\\&=\sum_{\mu}\frac{1}{C_{\mu}}\sum_{i}F_{\mu}|\psi_i\rangle\langle\psi_i|F_{\mu}^{\dagger}=R.\end{aligned}$$

By adding the projector $I-R$ to R_{μ}'s, we obtain a set of recovery operators (Kraus operators) satisfying the normalization condition. □

Remark 2. The distance of a stabilizer code can be defined as the smallest positive integer d such that the quantum error correction criteria is satisfied for all error combinations $E_b^{\dagger}E_a$ of weight in the range $1\leq w(E_b^{\dagger}E_a)<d$.

A code is called *nondegenerate*, if $\langle\psi_j|E_b^{\dagger}E_a|\psi_i\rangle=\delta_{ab}\delta_{ij}$ for all a,b,i and j. A code that is not nondegenerate is *degenerate*. For example, consider the 9-qubit code (Shor code) with the following stabilizer:

$$\begin{aligned}S=\big\langle&Z_1Z_2,Z_2Z_3,Z_4Z_5,Z_5Z_6,Z_7Z_8,Z_8Z_9,\\&X_1X_2X_3X_4X_5X_6,X_4X_5X_6X_7X_8X_9\big\rangle.\end{aligned}$$

It is a $[[9,1,3]]$ code with these codewords:

$$\begin{aligned}|0\rangle_L&=\frac{1}{\sqrt{8}}\big(|000\rangle+|111\rangle\big)\otimes\big(|000\rangle+|111\rangle\big)\\&\quad\otimes\big(|000\rangle+|111\rangle\big),\\|1\rangle_L&=\frac{1}{\sqrt{8}}\big(|000\rangle-|111\rangle\big)\otimes\big(|000\rangle-|111\rangle\big)\\&\quad\otimes\big(|000\rangle-|111\rangle\big).\end{aligned}$$

The Shor code is degenerate, because we cannot distinguish Z_1 and Z_2,

$$Z_1Z_2|\psi\rangle=|\psi\rangle\Longleftrightarrow Z_1|\psi\rangle=Z_2|\psi\rangle.$$

5.1.2 Syndrome extraction

Based on the property that every two Pauli products either commute or anti-commute, we will see how a stabilizer code detects and corrects errors. The corresponding *syndrome* of a given error is a bit string including which stabilizer generator commutes or anti-commutes with the error. Given an error E, its syndrome is denoted by $\mathrm{Syn}(E)$. For example, consider the 5-qubit code with the following stabilizer

$$S=\big\langle Z_1X_2X_3Z_4,Z_2X_3X_4Z_5,Z_1Z_3X_4X_5,X_1Z_2Z_4X_5\big\rangle.$$

The syndrome for the error X_2 is $(0\quad 1\quad 0\quad 1)$, where 0's indicate that the generators g_1,g_3 commute with X_2 and 1's indicate that the generators g_2,g_4 anti-commute with X_2.

Proposition 1. *Given a stabilizer code Q, there exists an error with any given syndrome.*

Proof. Let $S=\langle g_1,...,g_l\rangle$ be the stabilizer of Q. The syndrome of an error E is a bit string of length l. Therefore, $b=(b_1\ldots b_l)$ is the syndrome of E if and only if $b(g_i)Jb(E)^t=b_i$ for all i (Lemma 1). It gives a system of equations with l equations and $2n$ variables ($l\leq n$) which has a nonzero solution. □

Any code allows correction of a particular family of correctable errors. Given a stabilizer code Q with stabilizer S, error operators in S are all correctable. If the noise of the system under consideration includes only these errors, the code is called a *decoherence free* subspace. There is a large family $\mathcal{E}=\{E_{\alpha}\}$ of errors which are correctable by extracting the corresponding syndromes. It is shown that if for every product $E_{\alpha}E_{\beta}$ of two members of $\mathcal{E}$, either $E_{\alpha}E_{\beta}\in S$ or $E_{\alpha}E_{\beta}s=-sE_{\alpha}E_{\beta}$ for some $s\in S$ then $\mathcal{E}$ is correctable. Let $|\psi\rangle=\sum_i a_i|\psi_i\rangle$ be a general encoded state.

In the first case, E_{α} and E_{β} have the same syndrome, so are indistinguishable, but both are correctable because the common syndrome leads us to apply E_{α} as the corrective operator. If it was E_{α} which occured, this is well, while if E_{β} occured, the final state will be $E_{\alpha}E_{\beta}|\psi\rangle=|\psi\rangle$ which is also correct. This case is related to degenerate codes.

In the second case, either $E_{\alpha}s=sE_{\alpha},E_{\beta}s=-sE_{\beta}$, or $E_{\alpha}s=-sE_{\alpha},E_{\beta}s=sE_{\beta}$. It follows that E_{α} and E_{β} have different syndromes, thus they are distinguishable from each other. The noisy state is $\sum_{\alpha}(E_{\alpha}|\psi\rangle)\otimes|\phi_{\alpha}\rangle_E$. Quantum error correction determines the error syndrome with the help of ancilla qubits:

$$\begin{aligned}&|0\rangle_A\otimes\sum_{\alpha}(E_{\alpha}|\psi\rangle)\otimes|\phi_{\alpha}\rangle_E\\&\quad\mapsto\sum_{\alpha}|\mathrm{Syn}(E_{\alpha})\rangle_A\otimes(E_{\alpha}|\psi\rangle)\otimes|\phi_{\alpha}\rangle_E.\end{aligned}$$

By a projective measurement of the ancilla, the sum will be collapsed to a single term randomly $|\mathrm{Syn}(E_{\alpha})\rangle_A\otimes(E_{\alpha}|\psi\rangle)\otimes|\phi_{\alpha}\rangle_E$ and we will obtain $\mathrm{Syn}(E_{\alpha})$ as the measurement result. Since there is only one error with this syndrome, we are able to apply E_{α} to correct the error. This case is related to nondegenerate codes.

5.2 Symplectic structure

Matrix $M\in\mathbb{F}_2^{2n\times 2n}$ is called *symplectic*, if $MJM^t=J$. The set of all symplectic matrices in $\mathbb{F}_2^{2n\times 2n}$ is denoted by $\mathrm{Sp}(2n,\mathbb{F}_2)$, which is a group under matrix multiplication.

Lemma 4. *Up to a global phase, $\mathcal{C}_n/\mathcal{P}_n\simeq\mathrm{Sp}(2n,\mathbb{F}_2)$.*

Proof. For $\boldsymbol{a}=(\boldsymbol{a}_1\ \boldsymbol{a}_2)\in\mathbb{F}_2^{2n}$, where $\boldsymbol{a}_i=(a_i^1\ a_i^2\ \ldots\ a_i^n)$, let

$$\xi(\boldsymbol{a}) := \boldsymbol{X}^{\boldsymbol{a}_1}\boldsymbol{Z}^{\boldsymbol{a}_2} = \prod_{i=1}^{n} X_i^{a_1^i} \prod_{i=1}^{n} Z_i^{a_2^i}.$$

It follows that for every $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^{2n}$,

$$\xi(\boldsymbol{a})\xi(\boldsymbol{b}) = (-1)^{\langle \boldsymbol{b}_1,\, \boldsymbol{a}_2\rangle}\xi(\boldsymbol{a}+\boldsymbol{b}) = (-1)^{\boldsymbol{b}\begin{pmatrix}\boldsymbol{0} & I\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{a}^t}\xi(\boldsymbol{a}+\boldsymbol{b}),$$

and every $u \in \mathcal{C}_n$ satisfies $u\xi(\boldsymbol{a})u^\dagger = (-1)^{f(\boldsymbol{a})}\xi(g(\boldsymbol{a}))$ for some functions f and g. It turns out that

$$\begin{aligned}
&(-1)^{f(\boldsymbol{a}+\boldsymbol{b})}\xi(g(\boldsymbol{a}+\boldsymbol{b})) = u\xi(\boldsymbol{a}+\boldsymbol{b})u^\dagger\\
&= (-1)^{\boldsymbol{b}\begin{pmatrix}\boldsymbol{0} & I\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{a}^t} u\xi(\boldsymbol{a})u^\dagger u\xi(\boldsymbol{b})u^\dagger\\
&= (-1)^{f(\boldsymbol{a})+f(\boldsymbol{b})+\boldsymbol{b}\begin{pmatrix}\boldsymbol{0} & I\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{a}^t} \xi(g(\boldsymbol{a}))\xi(g(\boldsymbol{b}))\\
&= (-1)^{f(\boldsymbol{a})+f(\boldsymbol{b})+\boldsymbol{b}\begin{pmatrix}\boldsymbol{0} & I\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{a}^t+g(\boldsymbol{b})\begin{pmatrix}\boldsymbol{0} & I\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}g(\boldsymbol{a})^t} \xi(g(\boldsymbol{a})+g(\boldsymbol{b})).
\end{aligned}$$

From this equality, we have

$$\begin{aligned}
f(\boldsymbol{a}+\boldsymbol{b}) &= f(\boldsymbol{a}) + f(\boldsymbol{b}) + \boldsymbol{b}\begin{pmatrix}\boldsymbol{0} & I\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{a}^t\\
&\quad + g(\boldsymbol{b})\begin{pmatrix}\boldsymbol{0} & I\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}g(\boldsymbol{a})^t,\\
g(\boldsymbol{a}+\boldsymbol{b}) &= g(\boldsymbol{a}) + g(\boldsymbol{b}).
\end{aligned}$$

Therefore, $g(\boldsymbol{x}) = \boldsymbol{x}M$ for some $M \in \mathbb{F}_2^{2n\times 2n}$ and

$$f(\boldsymbol{x}) = \langle \boldsymbol{r}, \boldsymbol{x}\rangle + \boldsymbol{b}\begin{pmatrix}\boldsymbol{0} & I\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}\boldsymbol{a}^t + g(\boldsymbol{b})\begin{pmatrix}\boldsymbol{0} & I\\ \boldsymbol{0} & \boldsymbol{0}\end{pmatrix}g(\boldsymbol{a})^t,$$

for some $\boldsymbol{r} \in \mathbb{F}_2^{2n}$. Let $\langle \boldsymbol{x}, \boldsymbol{y}\rangle_{\mathrm{s}} := \boldsymbol{x}J\boldsymbol{y}^t$ be the symplectic inner product. We note that $\xi(\boldsymbol{x})$ and $\xi(\boldsymbol{y})$ commute (anti-commute) if and only if $\langle \boldsymbol{x}, \boldsymbol{y}\rangle_{\mathrm{s}} = 0(1)$. Given unitary $u \in \mathcal{C}_n$, conjugating by u $(\sigma \mapsto u\sigma u^\dagger)$ preserves commutation (anti-commutation) of $\xi(\boldsymbol{x})$ and $\xi(\boldsymbol{y})$, then its corresponding matrix M preserves the symplectic inner product, i.e., $\boldsymbol{x}J\boldsymbol{y}^t = \boldsymbol{x}MJ(\boldsymbol{y}M)^t = \boldsymbol{x}MJM^t\boldsymbol{y}^t$ for every $\boldsymbol{x}$ and $\boldsymbol{y}$. Hence, $MJM^t = J$, i.e., $M \in \mathrm{Sp}(2n, \mathbb{F}_2)$, and $h : \mathcal{C}_n \to \mathrm{Sp}(2n, \mathbb{F}_2)$ which maps u onto M defines a group homomorphism. It is clear that $\mathcal{P}_n \subset \mathrm{Ker}(h) = \{u \in \mathcal{C}_n : uvu^\dagger = \pm v, \forall v \in \mathcal{P}_n\}$. Let $u \in \mathrm{Ker}(h)$, then $uX_ju^\dagger = \pm X_j$ and $uZ_ju^\dagger = \pm Z_j$ for all j. The sign changes reveal that which of the Pauli operators I, X, Y and Z is being to qubit j by u, call this operator v_j. Together these operators we construct the Pauli product $v = \prod_{j=1}^n v_j$ which is equal to u, because they perform the same thing when conjugating every generator of $\mathcal{P}_n = \langle X_1, Z_1, ..., X_n, Z_n\rangle$. □

Given $k \le n$, the *k-trivial stabilizer code* on n qubits is defined by

$$T_k = \{|0\rangle^{\otimes(n-k)} \otimes |\phi\rangle : |\phi\rangle \in (\mathbb{C}^2)^{\otimes k}\}.$$

Theorem 5. *For any stabilizer code $Q \in [[n, k]]$, there exists a unitary operator $u \in \mathcal{C}_n$ such that $Q = uT_k$. In other words, Q and T_k are (Clifford) unitarily equivalent.*

Proof. Given code Q stabilized by $S = \langle g_1, ..., g_{n-k}\rangle$. We take into account that the stabilizer of T_k is generated by $Z_1, ..., Z_{n-k}$. We need to find a unitary u such that $uZ_iu^\dagger = g_i$ for all i. In general, this unitary u is not unique since we can redefine it by any $v \in \mathcal{C}_n$ which acts trivially on T_k. However, any choice of stabilizer basis of Q induces a u. In fact, a choice of logical basis $|\bar{x}\rangle$ corresponds to a full completion $g_1, ..., g_{n-k}, g_{n-k+1}, ..., g_n$ of the generators and the logical basis is determined by the eigenvalues of $g_{n-k+1}, ..., g_n$. The unitary u defined by $uZ_iu^\dagger = g_i$ for $i = 1, ..., n$ is a Clifford operator because the Pauli products on the left and right hand side are fully commuting sets. This unitary u transforms input states as follows:

$$\begin{aligned}
|0\rangle^{\otimes(n-k)} \otimes |\phi\rangle &= \sum_{x\in\mathbb{F}_2^k} \lambda_x |0\rangle^{\otimes(n-k)} \otimes |x\rangle\\
&\mapsto \sum_{x\in\mathbb{F}_2^k} \lambda_x |0\rangle^{\otimes(n-k)} \otimes |\bar{x}\rangle.
\end{aligned}$$

□

In classical coding theory, it is usual to use finite fields larger than $\mathbb{F}_2$. The simplest example is $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ with $\omega^3 = 1, \omega^2 = \omega + 1$. It is a field of characteristic 2 with the following two operations: 1) Conjugation: $\bar{0} = 0, \bar{1} = 1, \bar{\omega} = \omega^2, \bar{\omega^2} = \omega$. 2) Trace: $\mathrm{Tr} : \mathbb{F}_4 \to \mathbb{F}_2, x \mapsto x + \bar{x}$. Let $\lambda : \mathbb{F}_2^{2n} \to \mathbb{F}_4^n$ be a mapping which sends each $\nu = (a|b)$ to $\lambda(\nu) = a\omega + b\bar{\omega}$. For $\nu = (a|b)$ and $\nu' = (a'|b')$ in $\mathbb{F}_2^{2n}$,

$$\begin{aligned}
\mathrm{Tr}(\langle \lambda(\nu), \overline{\lambda(\nu')}\rangle) &= \mathrm{Tr}\big(\langle (a\omega + b\bar{\omega}), (a'\bar{\omega} + b'\omega)\rangle\big)\\
&= \langle a, a'\rangle \mathrm{Tr}(1) + \langle a, b'\rangle \mathrm{Tr}(\bar{\omega})\\
&\quad + \langle b, a'\rangle \mathrm{Tr}(\omega) + \langle b, b'\rangle \mathrm{Tr}(1)\\
&= \langle a, b'\rangle + \langle b, a'\rangle = \nu J\nu'^t = \langle \nu, \nu'\rangle_{\mathrm{s}}.
\end{aligned}$$

Here, the trace inner product turns into the symplectic inner product. The Pauli operators I, X, Y and Z are associated with $0, 1, \omega^2$ and ω, respectively. Given a linear code over $\mathbb{F}_4$ with parity check matrix P_c. Since $\mathbb{F}_4 = \{a + b\omega : a, b \in \{0, 1\}\}$, then any vector in the dual space of the code can be generated by summing together selected rows of P_c, each multiplied by ω. It is shown that the 5-qubit code (over $\mathbb{F}_2$) is derived from the Hamming code $[5, 3, 3]$ over $\mathbb{F}_4$. In this way, we need to find Pauli products associated with the rows of P_c and ωP_c as follows:

$$\begin{aligned}
&P_c = \begin{pmatrix}1 & \omega & \omega & 1 & 0\\ 0 & 1 & \omega & \omega & 1\end{pmatrix},\\
&r_1 = (1 \quad \omega \quad \omega \quad 1 \quad 0) \longrightarrow g_1 = X_1Z_2Z_3X_4I_5,\\
&r_2 = (0 \quad 1 \quad \omega \quad \omega \quad 1) \longrightarrow g_2 = I_1X_2Z_3Z_4X_5,\\
&\omega r_1 = (\omega \quad \omega^2 \quad \omega^2 \quad \omega \quad 0) \longrightarrow g_3 = Z_1Y_2Y_3Z_4I_5,\\
&\omega r_2 = (0 \quad \omega \quad \omega^2 \quad \omega^2 \quad \omega) \longrightarrow g_4 = I_1Z_2Y_3Y_4Z_5.
\end{aligned}$$

It follows that $S = \langle g_1', g_2', g_3', g_4'\rangle$ with $g_1' := g_3g_2 = Z_1Z_2X_3X_5$, $g_2' := g_4g_1 = X_1X_3Z_4Z_5$, $g_3' := g_1$, and $g_4' := g_2$ is the stabilizer for the 5-qubit code.

5.3 Graph codes

Let $\mathcal{G}$ be a graph with a set of $\mathcal{V}$ of n vertices and a collection $\mathfrak{E}$ of edges. We associate the vertices to the numbers $1, 2, ..., n$. We are only interested in graphs without loops, i.e., there are no edges of the form (i, i). The *graph state* $|\mathcal{G}\rangle$ is defined as the stabilizer state stabilized by the following Pauli products:

$$g_i := X_i \prod_{j \in N(i)} Z_j \quad \forall i \in \mathcal{V}, \tag{9}$$

where $N(i) = \{j \in \mathcal{V} : (i, j) \in \mathfrak{E}\}$. The corresponding parity check matrix for generators of a graph state is in the standard form, i.e., $G = (I|A)$. Let CP_{ij} be the controlled phase operator (gate) between qubits i and j,

$$CP_{ij} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

and $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, the graph state $|\mathcal{G}\rangle$ can be defined as [24]

$$|\mathcal{G}\rangle = \prod_{(i,j)\in\mathfrak{E}} CP_{ij}|+\rangle^{\otimes n}. \tag{10}$$

Each graph state $|\mathcal{G}\rangle$ corresponds uniquely to a graph, i.e., two different graphs $\mathcal{G} = (\mathcal{V}, \mathfrak{E})$ and $\mathcal{G}' = (\mathcal{V}, \mathfrak{E}')$ cannot describe the same graph state, because

$$\begin{aligned} |+\rangle^{\otimes n} &= \prod_{(i,j)\in\mathfrak{E}'} CP_{ij}|\mathcal{G}'\rangle = \prod_{(i,j)\in\mathfrak{E}'} CP_{ij}|\mathcal{G}\rangle \\ &= \prod_{(i,j)\in\mathfrak{E}'} CP_{ij} \prod_{(i,j)\in\mathfrak{E}} CP_{ij}|+\rangle^{\otimes n} \\ &= \prod_{(i,j)\in\mathfrak{E}+\mathfrak{E}'} CP_{ij}|+\rangle^{\otimes n}, \end{aligned}$$

where $\mathfrak{E} + \mathfrak{E}' \neq \emptyset$ denotes the symmetric difference of the edge sets, which is a contradiction. Another fact is that for any stabilizer state $|\mathcal{S}\rangle$, there is a graph state $|\mathcal{G}\rangle$ and a unitary operator $u \in \mathcal{C}_1^{\otimes n}$ such that $|\mathcal{S}\rangle = u|\mathcal{G}\rangle$ (local Clifford equivalence) [25].

Given a graph $\mathcal{G}$ and a classical linear code $\mathfrak{C}$, a *graph code* $(\mathcal{G}, \mathfrak{C})$ is defined as the linear span of the states $\boldsymbol{Z}^{\boldsymbol{a}}|\mathcal{G}\rangle$, where $\boldsymbol{a}$ is any codeword in $\mathfrak{C}$. The simplest example of a graph code is yielded by a trivial graph with no edges. The distance of this code is 1 (see Remark 2).

Theorem 6. *Given a graph $\mathcal{G} = (\mathcal{V}, \mathfrak{E})$ and a linear code $\mathfrak{C} \in [n, k]$, let $Q = (\mathcal{G}, \mathfrak{C})$ be the associated graph code. Then $Q \in [[n, k]]$.*

Proof. Suppose that $Q \in [[n, k']]$. We take into account that

$$CP_{ij} = \tfrac{1}{2}(I + Z_i + Z_j - Z_iZ_j),$$

then Z_l's commute with CP_{ij}'s. For every $\boldsymbol{a} = (a_1, ..., a_n) \in \mathfrak{C}$, we define $|\boldsymbol{a}\rangle := \boldsymbol{Z}^{\boldsymbol{a}}|\mathcal{G}\rangle$, therefore by applying (10)

$$|\boldsymbol{a}\rangle = \prod_{l=1}^{n} Z_l^{a_l} \prod_{(i,j)\in\mathfrak{E}} CP_{ij}|+\rangle^{\otimes n} = \prod_{(i,j)\in\mathfrak{E}} CP_{ij} \prod_{l=1}^{n} Z_l^{a_l}|+\rangle^{\otimes n}.$$

Since $|\mathfrak{C}| = 2^k$ and $Z_l|+\rangle = |-\rangle$ where $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, then the set of states of the form $\boldsymbol{Z}^{\boldsymbol{a}}|+\rangle^{\otimes n}$ constitutes an orthonormal basis of 2^k elements in which each qubit is $|+\rangle$ or $|-\rangle$. As $\prod_{(i,j)\in\mathfrak{E}} CP_{ij}$ is a unitary operator, it maps one orthonormal basis to another orthonormal basis, therefore $\dim(Q) = 2^k$ and $k' = k$. □

We recall that the *support of a vector* $\nu = (\nu_1, ..., \nu_n)$ is the set of indices i for which $\nu_i \neq 0$ and is denoted by $\mathrm{Supp}(\nu)$. After this note, we will construct a set of stabilizer generators for a graph code as follows.

Theorem 7. *Given a graph $\mathcal{G}$ and a linear code $\mathfrak{C} \in [n, k]$, let ${\boldsymbol{a}_1}^{\perp}, ..., {\boldsymbol{a}_{n-k}}^{\perp}$ be a minimal weight generating set for the dual code $\mathfrak{C}^{\perp}$. The graph code $(\mathcal{G}, \mathfrak{C})$ is a stabilizer code with the following stabilizer generators*

$$S_j = \prod_{i\in\mathrm{Supp}({\boldsymbol{a}_j}^{\perp})} g_i,$$

where g_i is defined in Eq. (9).

Proof. Let S be the stabilizer for $Q = (\mathcal{G}, \mathfrak{C})$. We show that $S = \langle S_1, ..., S_{n-k}\rangle$. Independence of S_i's follows from the linear independence of the binary vectors $\boldsymbol{a}_i^{\perp}$'s. Since $[g_i, g_j] = 0$ for all i and j, then S_i's commute. It remains to show that for every codeword $\boldsymbol{a} \in \mathfrak{C}$, the state $\boldsymbol{Z}^{\boldsymbol{a}}|\mathcal{G}\rangle$ is stabilized by S_j's. For every j, we can rewrite S_j as follows:

$$S_j = \prod_{i\in\mathrm{Supp}(\boldsymbol{a}_j^{\perp})} g_i = (-1)^{\alpha}\boldsymbol{Z}^{\boldsymbol{b}}\Big(\prod_{i\in\mathrm{Supp}(\boldsymbol{a}_j^{\perp})} X_i\Big), \tag{11}$$

where $\alpha = 0$ or 1, and $\boldsymbol{b}$ is a binary vector. Since $\boldsymbol{a}_j^{\perp} \in \mathfrak{C}^{\perp}$, then $\boldsymbol{Z}^{\boldsymbol{a}}$ and $\prod_{i\in\mathrm{Supp}(\boldsymbol{a}_j^{\perp})} X_i$ commute, thus by applying Eq. (11) we have

$$\begin{aligned} S_j\boldsymbol{Z}^{\boldsymbol{a}}|\mathcal{G}\rangle &= (-1)^{\alpha}\boldsymbol{Z}^{\boldsymbol{b}}\Big(\prod_{i\in\mathrm{Supp}(\boldsymbol{a}_j^{\perp})} X_i\Big)\boldsymbol{Z}^{\boldsymbol{a}}|\mathcal{G}\rangle \\ &= \boldsymbol{Z}^{\boldsymbol{a}} \prod_{i\in\mathrm{Supp}(\boldsymbol{a}_j^{\perp})} g_i|\mathcal{G}\rangle = \boldsymbol{Z}^{\boldsymbol{a}}|\mathcal{G}\rangle. \end{aligned}$$

□

Graph codes play a key role in quantum technologies by yielding considerable protection against qubit loss, a dominant noise mechanism [26].

5.4 Cleaning lemma

Given an $[[n, k]]$ stabilizer code with stabilizer S. An operator (Pauli product) is said *to be supported* on a region M (a subset of n qubits) if it acts trivially on M^c (the complement of M). The *support of an operator* u is the minimal region on which u is supported and is

denoted by $\mathrm{Supp}(u)$. According to Lemma 1, we can regard $\mathcal{P}_n$ as an $2n$-dimensional vector space on $\mathbb{F}_2$. We say a set of *independent* logical operators to mean one that maps to a linear independent set in the quotient vector space $\mathcal{P}_n/S$. We recall that two vectors are orthogonal (with respect to the symplectic inner product) if and only if the corresponding operators commute, thus $\mathcal{L} = S^{\perp}$ where $S^{\perp}$ is the orthogonal complement of S in $\mathcal{P}_n$.

Lemma 5. *Let $l(M)$ and $l(M^c)$ be the number of independent logical operators that can be supported on M and M^c, respectively. Then $l(M) + l(M^c) = 2k$.*

Proof. Let $\mathcal{P}_M$ be the subspace of $\mathcal{P}_n$ which is supported on M. We can write S as $S = S_M \oplus S_{M^c} \oplus \tilde{S}$, where $S_M = S \cap \mathcal{P}_M$ and $S_{M^c} = S \cap \mathcal{P}_{M^c}$ are the subspaces of S which are supported on M and M^c, respectively and $\tilde{S}$ includes whatever remains beyond $S_M \oplus S_{M^c}$. Let us define the restriction of a vector $\boldsymbol{c} = (c_1, ..., c_{2n})$ to M as $\boldsymbol{c}|_M := \sum_{i\in M}(c_i \boldsymbol{e}^i + c_{n+i}\boldsymbol{e}^{n+i})$, where $\{\boldsymbol{e}^i\}$ is the standard basis for $\mathcal{P}_n$. Let $\tilde{S}|_M$ denote the restriction of $\tilde{S}$ to M. We take into account that linearly independent vectors in $S_M + \tilde{S}$ remain linearly independent in $S_M + \tilde{S}|_M$, otherwise a nontrivial linear combination of the vectors would have a trivial restriction to M, thus would be in S_{M^c}. Since S_{M^c} is trivially orthogonal to $\mathcal{P}_M$, then $(S^{\perp})_M$ is the orthogonal complement of $(S_M + \tilde{S})|_M$ in $\mathcal{P}_M$. Hence,

$$\begin{aligned}\dim (S^{\perp})_M &= \dim \mathcal{P}_M - \dim(S_M + \tilde{S}|_M) \\ &= \dim \mathcal{P}_M - \dim S_M - \dim \tilde{S}. \end{aligned} \tag{12}$$

Similarly by replacing M with M^c we have

$$\begin{aligned}\dim (S^{\perp})_{M^c} &= \dim \mathcal{P}_{M^c} - \dim(S_{M^c} + \tilde{S}|_{M^c}) \\ &= \dim \mathcal{P}_{M^c} - \dim S_{M^c} - \dim \tilde{S}. \end{aligned} \tag{13}$$

Since logical operators supported on M (M^c) are elements of $\mathcal{P}_M$ ($\mathcal{P}_{M^c}$) which commute with S and are not contained in S, then by applying Eqs. (12) and (13)

$$\begin{aligned} l(M) &= \dim (S^{\perp})_M - \dim S_M \\ &= \dim \mathcal{P}_M - 2\dim S_M - \dim \tilde{S}, \\ l(M^c) &= \dim (S^{\perp})_{M^c} - \dim S_{M^c} \\ &= \dim \mathcal{P}_{M^c} - 2\dim S_{M^c} - \dim \tilde{S}. \end{aligned}$$

It follows that

$$\begin{aligned} l(M) + l(M^c) &= \dim \mathcal{P}_M + \dim \mathcal{P}_{M^c} - 2(\dim S_M \\ &\quad + \dim S_{M^c} + \dim \tilde{S}) \\ &= \dim \mathcal{P}_n - 2\dim S = 2n - 2(n-k) = 2k. \end{aligned}$$

□

For a logical operator u, we say that u *can be cleaned on* M, if there exists a logically equivalent operator u', i.e., $u' = us$ where $s \in S$, such that u' can be supported on M^c. Now we are ready to present the cleaning lemma [27, 28] as follows.

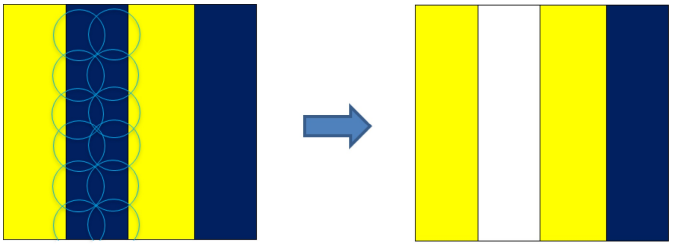


Fig. 2 Applying the cleaning lemma.

Corollary 3. *Let M be a region which does not support any nontrivial logical operator. Then any logical operator can be cleaned on M.*

Proof. The assumption means that $l(M) = 0$. Hence, by applying Lemma 5, it follows that $l(M^c) = 2k$. Therefore, any logical operator may be supported on M^c. It means that any logical operator can be cleaned on M. In other words, for any logical operator u, we can choose an element $s = \prod_{i\in\Sigma(M)} g_i^{x_i} \in S$, with $\Sigma(M) = \{i : \mathrm{Supp}(g_i) \cap M \neq \emptyset\}$ and $x_i \in \{0, 1\}$, such that $u' = us$ acts trivially on M. □

Given a lattice $\Lambda = \{1, ..., L\}^N$ (L is sufficiently large) we say that a stabilizer code Q with stabilizer $S = \langle g_1, ..., g_m\rangle$ is *embeddable* into Λ, if we can associate the qubits to vertices of Λ such that each g_i is supported only on one hypercube, say of size 1, of Λ.

Theorem 8. *Given an embeddable stabilizer code $Q \in [[n, k, d]]$ in an N-dimensional lattice, $d = O(n^{1-\frac{1}{N}})$.*

Proof. We will prove the theorem for two-dimensional lattices, the higher dimensional case will be clear from $N = 2$. Suppose that for some $M \gg 1$

$$d \geq M\sqrt{n}. \tag{14}$$

For sufficiently large L, we can divide Λ into an even number of vertical strips, say r strips, of width at most $\frac{M}{2}$ but still larger than 1. Let u be a nontrivial logical operator on Λ. According to Corollary 3, each vertical strip can be cleaned out by applying the generators whose supports overlap with that strip. We note that these supports are located on that strip or adjacent strips, but not on any other strips (Fig. 2).

By repeating this process, all even strips will be cleaned out and we obtain a logical operator u' which is supported only on odd strips $u' = u'_1 u'_3 ... u'_{r-1}$, where u'_i is a Pauli product which is supported on the i-th strip. Since each generator g_j overlaps with at most one odd strip and $u' \in N(S)$, then $u'_i \in N(S)$ for all $i = 1, 3, ..., r-1$. Since $u' \notin S$, there is at least one odd strip i such that $u'_i \notin S$ which means u'_i is a nontrivial logical operator. But $w(u'_i) < (\frac{M}{2})L = (\frac{M}{2})\sqrt{n}$ which is a contradiction with Eq. (14). Hence, $d = O(\sqrt{n})$. □

5.5 Generalization

The notion of stabilizer code can be generalized to

qudits, i.e., d-level systems, where d is a prime number. Here, the system has only a finite number of accessible states (degrees of freedom), thus the phase space needs to be discrete. In this case, the Hilbert spaces of constituents are $\mathbb{C}^d$ with the standard basis $|0\rangle, ..., |d-1\rangle$. The *shift* operator and the *clock* operator are defined as follows:

$$X|j\rangle := |j+1\rangle, \quad Z|j\rangle := \mathrm{e}^{\frac{2\pi \mathrm{i}}{d}j}|j\rangle,$$

and modulo-d arithmetic is used. These operators satisfy $X^d = Z^d = I$. We associate with each point $(x,p) \in \mathbb{F}_d^2$ in phase space a Weyl operator according $T(x,p) := X^x Z^p$. The Weyl operators can be conceived as generalized Pauli products. They satisfy the Weyl commutation relations:

$$T(x,p)T(x',p') = e^{\frac{-2\pi i}{d}p'x}\, T(x+x', p+p').$$

It follows that two Weyl operators $T(x,p)$ and $T(x',p')$ commute if and only if the standard symplectic inner product vanishes

$$\big[(x,p),(x',p')\big] := (x,p)\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}(x',p')^t = px' - xp'.$$

For n qudits, we can encounter (position and momentum) coordinates $(x_1, p_1, ..., x_n, p_n)$ in phase space with $\boldsymbol{x} = (x_1, ..., x_n), \boldsymbol{p} = (p_1, ..., p_n) \in \mathbb{F}_d^n$. The above inner product gives rise to the following form

$$\big[(\boldsymbol{x},\boldsymbol{p}),(\boldsymbol{x}',\boldsymbol{p}')\big] = (\boldsymbol{x},\boldsymbol{p})\Omega(\boldsymbol{x}',\boldsymbol{p}')^t, \tag{15}$$

where $\Omega := \bigoplus_{j=1}^{n}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$. The *generalized Weyl operator* is defined by

$$\boldsymbol{T}(\boldsymbol{x},\boldsymbol{p}) := \bigotimes_{j=1}^{n} T(x_j, p_j).$$

Let $\mathfrak{W}(\boldsymbol{x},\boldsymbol{p}) := \mathrm{e}^{\frac{-\pi \mathrm{i}}{d}\langle \boldsymbol{x},\boldsymbol{p}\rangle}\boldsymbol{T}(\boldsymbol{x},\boldsymbol{p})$. An *isotropic subspace* $\mathfrak{V} \subset \mathbb{F}_d^{2n}$ is a subspace on which the inner product of Eq. (15) vanishes. A *character* χ is a map from $\mathfrak{V}$ into the circle group $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. A *generalized stabilizer code* associated with $\mathfrak{V}$ and χ is defined as follows

$$Q = \big\{|\psi\rangle \in (\mathbb{C}^d)^{\otimes n} : \chi^*(\boldsymbol{x},\boldsymbol{p})\mathfrak{W}(\boldsymbol{x},\boldsymbol{p})|\psi\rangle = |\psi\rangle, \forall(\boldsymbol{x},\boldsymbol{p}) \in \mathfrak{V}\big\}.$$

The *generalized Clifford group* is defined as the set of unitary operators u that map Weyl operators onto Weyl operators under conjugation, i.e.,

$$u\mathfrak{W}(\boldsymbol{x},\boldsymbol{p})u^\dagger \propto \mathfrak{W}(\mathfrak{G}(\boldsymbol{x},\boldsymbol{p})),$$

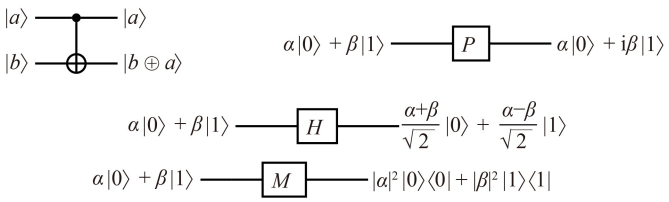
where $\mathfrak{G}$ belongs to the symplectic group induced by Eq. (15) and $\propto$ is the symbol of proportionality.

Remark 3. We take into account that the direct analog of stabilizer states makes sense in the setting of continuous Weyl systems by describing singular states within an algebraic approach [29].

In the following section, we study stabilizer circuits as a very important class of quantum circuits. In fact, they are sufficient to implement many quantum algorithms and protocols.

6 Stabilizer circuits

In quantum computation, it is more convenient to work with circuit model rather than matrix equivalent representation. For example, four gates are allowed in the stabilizer formalism, including controlled NOT (**CNOT**), phase (***P***), Hadamard (***H***) and measurement (***M***) are given below:



where $\oplus$ is the addition modulo 2 and

$$\mathbf{CNOT} = \frac{1}{2}(I_1I_2 + Z_1I_2 + I_1X_2 - Z_1X_2),$$

$$\boldsymbol{P} = \frac{1}{\sqrt{2}}(I - \mathrm{i}Z), \quad \boldsymbol{H} = \frac{1}{\sqrt{2}}(X+Z).$$

6.1 Simulating the stabilizer gates

Up to a global phase, the Clifford group $\mathcal{C}_n$ is generated by one and two qubit gates in the set $\{\boldsymbol{H}, \boldsymbol{P}, \mathbf{CNOT}\}$, which are called the *Clifford gates* [30]. Let f and g be two positive functions, we write $f \in O(g)$ if $\limsup_{n\to\infty}\frac{f(n)}{g(n)} < \infty$, and $f \in \Theta(g)$ if $\limsup_{n\to\infty}\frac{f(n)}{g(n)} < \infty$ and $\liminf_{n\to\infty}\frac{f(n)}{g(n)} > 0$.

Theorem 9. *Simulating a Clifford gate on an n-qubit stabilizer state requires $\Theta(n)$ time, while a measurement gate is simulated in $O(n^2)$ time for random outcomes and in $O(n^3)$ time for deterministic outcomes.*

Proof. Given an n-qubit stabilizer state $|\psi\rangle$ with stabilizer S, we apply the idea of representing $|\psi\rangle$ by a *stabilizer matrix* $\mathfrak{M}$ whose rows are a set of generators of S. Accordingly, any computational basis state can be represented as follows, where signs $\pm$ denote global phases ± 1 for the respective generator,

$$\begin{matrix}\pm\\ \pm\\ \pm\\ \vdots\\ \pm\end{matrix}\begin{pmatrix} Z_1 & I & I & \dots & I\\ I & Z_2 & I & \dots & I\\ I & I & Z_3 & \dots & I\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ I & I & \dots & I & Z_n\end{pmatrix}.$$

By simulating a Clifford gate u on $|\psi\rangle$, g_i, the i-th row of $\mathfrak{M}$, is mapped to $ug_iu^\dagger$, hence at most two columns of $\mathfrak{M}$ are updated. Therefore, u is simulated in $\Theta(n)$ time. We note that each qubit in $|\psi\rangle$ is either in a $|0\rangle(|1\rangle)$ state, *deterministic outcome*, or in an unbiased superposition of both states, *random outcome*. In the case of random outcome, we flip an unbiased coin to decide the outcome $x \in \{0,1\}$ and then update $\mathfrak{M}$ to match the outcome. Let g_j be a row in $\mathfrak{M}$ with an $X(Y)$ operator in its j-th position. The global phase of Z_j is set to $+1(-1)$ if $x = 0(1)$. Based on the fact that g_j and Z_j anti-commute, if any other rows in $\mathfrak{M}$ anti-commute with Z_j, we multiply them by g_j to make them commute with Z_j. After that, we replace g_j with Z_j. This process needs up to n row multiplications, then the overall runtime is $O(n^2)$. In the case of deterministic outcome, we need to find out whether the qubit is in the $|0\rangle(|1\rangle)$ state. In other words, whether the qubit is stabilized by $Z(-Z)$. In this way, we can perform Gaussian elimination to convert $\mathfrak{M}$ into a *row-echelon form* as follows:

$$\left(\begin{array}{cccc} X & X & & \mathfrak{A}_1 \\ & \ddots & & \\ & \mathfrak{A}_2 & & X \\ \hline Z & & & \\ & Z & & \mathfrak{A}_3 \\ & & \ddots & \\ & \mathfrak{A}_4 & & Z \end{array}\right),$$

where entries in $\mathfrak{A}_1$ (upper X-diagonal) are I, X, Y or Z, entries in $\mathfrak{A}_2$ (lower X-diagonal) and $\mathfrak{A}_3$ (upper Z-diagonal) are I or Z, and entries in $\mathfrak{A}_4$ (lower Z-diagonal) are only I. This process removes redundant operators from $\mathfrak{M}$, then it is possible to identify the row as Z_j. The $\pm$ phase of this row decides the outcome of the measurement. Since the Gaussian elimination process takes $O(n^3)$ time, thus the runtime is $O(n^3)$. □

6.2 Knill–Gottesman theorem

Given a quantum circuit $\mathcal{U}$ with n input qubits as one bit string, e.g., $|0\rangle^{\otimes n}$, by measuring the qubits, we would read out some sample bits $\varphi \in \{0,1\}^n$, with probability $\mathbb{P}(\varphi) = |\langle\varphi|\tau\rangle|^2$, where $|\tau\rangle = \mathcal{U}|0\rangle^{\otimes n}$. A *classical simulation* of a quantum circuit is the process of sampling from the output distribution efficiently using a classical probabilistic computer. By simulating a circuit, we will obtain an outcome φ that is in accordance with the probability distribution $\mathbb{P}(\varphi)$.

Theorem 10. (Knill–Gottesman theorem [16]) *Any quantum circuit that applies only the following elements can be simulated efficiently (in polynomial time) on a classical probabilistic computer.*

- *Preparation of qubits in computational basis states;*
- *Quantum gates from $\mathcal{C}_n$;*
- *Measurements in the computational basis.*

Proof. Without loss of generality, we start with the state $|0\rangle^{\otimes n}$ which is a stabilizer state with stabilizer $S = \langle Z_1, Z_2, ..., Z_n\rangle$. Let u be a generator of $\mathcal{C}_n$ and $|\psi'\rangle = u|\psi\rangle$. It follows that $|\psi'\rangle$ is a stabilizer state with stabilizer $uSu^\dagger = \langle uZ_1u^\dagger, uZ_2u^\dagger, ..., uZ_nu^\dagger\rangle$. Implementing a generator u implies updating the n generators which describe the initial state. This step requires $O(n^2)$ operations on a classical computer [30]. If our circuit is a product of m terms, each a generator of $\mathcal{C}_n$, then the computation can be simulated by a classical computer in $O(mn^2)$ time. □

A circuit satisfying the conditions of Theorem 10 is called a *stabilizer circuit*. Stabilizer circuits refer to quantum circuits including all of the four types of stabilizer gates, while *unitary* stabilizer circuits consist of only the Clifford gates. By adding any non-Clifford gate to the set of Clifford gates, we obtain a set of universal gates for quantum computation, while stabilizer circuits are probably not even universal for classical computation [30]. From Theorem 10, it follows that quantum algorithms employing the entanglement created by Clifford gates do not give any advantage over classical computers.

6.3 Tableau representation

Let $|\psi\rangle$ be an n-qubit stabilizer state with stabilizer $S = \langle g_1, g_2, ..., g_n\rangle$. We may write $S = \langle \widetilde{Z}_1, \widetilde{Z}_2, ..., \widetilde{Z}_n\rangle$, where $\widetilde{Z}_i$ acts on $|\psi\rangle$ just as Z_i acts on $|0\rangle^{\otimes n}$. In other words, we can think of the generators as surrogate Z operators. The operators $\widetilde{Z}_i$'s are called the *canonical Z operators* on a set of virtual qubits (syndrome qubits).

A *destabilizer (group)* D associated with a stabilizer $S = \langle g_1, g_2, ..., g_k\rangle$, is a stabilizer of $\mathcal{P}_n$, generated as $D = \langle d_1, d_2, ..., d_k\rangle$ such that for each i,

$$\{d_i, g_i\} = 0, \quad [d_i, g_j] = 0 \ \ \forall j \neq i.$$

Just as stabilizer generators can be thought of as canonical Z operators, destabilizer generators can be thought of as canonical X operators.

Let S be a stabilizer of $\mathcal{P}_n$ with n generators. A *full tableau* is a pair $\mathfrak{T} = (S, D)$, where D is a corresponding destabilizer.

Proposition 2. *Given a full tableau $\mathfrak{T} = (S, D)$, every $u \in \mathcal{P}_n$ can be decomposed as $u = i^k\mathfrak{d}s$ in $O(n^2)$ time, where $k \in \{0,1,2,3\}$, $\mathfrak{d} \in D$ and $s \in S$.*

Proof. Since $\mathfrak{T}$ is a full tableau, then generators of $S(D)$ are n canonical $Z(X)$ operators and up to a global phase, they can together generate $\mathcal{P}_n$. Therefore, such a decomposition exists. Given $u \in \mathcal{P}_n$, $g_j(d_j)$ is in the factorization of $s(\mathfrak{d})$ if and only if $\{u, d_j\} = 0$ ($\{u, g_j\} = 0$). We note that checking each of the $2n$ anti-commutation relations takes $O(n)$ time. After finding $\mathfrak{d}$ and s, we compare the phases of $\mathfrak{d}s$ and u to find k, which gives the desired decomposition in $O(n^2)$ time. □

The matrix representation of a full tableau $\mathfrak{T} = (S, D)$ is an $2n \times (2n+1)$ matrix $\mathcal{T}$ as follows:

$$\mathcal{T}=\left(\begin{array}{c|c|c} b_1(d_1) & b_2(d_1) & \alpha_1 \\ \vdots & \vdots & \vdots \\ b_1(d_n) & b_2(d_n) & \alpha_n \\ \hline b_1(g_1) & b_2(g_1) & \alpha_{n+1} \\ \vdots & \vdots & \vdots \\ b_1(g_n) & b_2(g_n) & \alpha_{2n} \end{array}\right),$$

where $\alpha_i = 0(1)$ if the global phase of the i-th generator is 1(–1). The standard initial tableau $\mathcal{I}$ is the following matrix,

$$\mathcal{I}=\left(\begin{array}{c|c|c} I & 0 & 0 \\ & & \vdots \\ & & 0 \\ \hline 0 & I & 0 \\ & & \vdots \\ & & 0 \end{array}\right).$$

We say that two n-qubit unitary stabilizer circuits $\mathcal{U}_1$ and $\mathcal{U}_2$ are *equivalent*, if the final states of them are equal, i.e., $\mathcal{U}_1(|\psi\rangle) = \mathcal{U}_2(|\psi\rangle)$ for all stabilizer states $|\psi\rangle$. By applying linearity, it follows that two equivalent stabilizer circuits have the same action on all states. In addition, there is a one-to-one correspondence between unitary stabilizer circuits and tableaus. That means, given a tableau matrix $\mathcal{T}$, there is a unitary stabilizer circuit $\mathcal{U}$ such that $\mathcal{T}$ is the final tableau when $\mathcal{U}$ is run on $\mathcal{I}$. This fact is based on a key theorem which says any unitary stabilizer circuit has an equivalent circuit in canonical form, i.e., it consists of 11 rounds in the following sequence [16],

$$\boldsymbol{H}-\textbf{CNOT}-\boldsymbol{P}-\textbf{CNOT}-\boldsymbol{P}-\textbf{CNOT}$$
$$-\boldsymbol{H}-\boldsymbol{P}-\textbf{CNOT}-\boldsymbol{P}-\textbf{CNOT}.$$

Corollary 4. *An n-qubit state $|\psi\rangle$ is a stabilizer state if and only if it can be obtained from $|0\rangle^{\otimes n}$ by a stabilizer circuit.*

Proof. Given a stabilizer state $|\psi\rangle$, let $\mathcal{T}$ be its tableau matrix and $\mathcal{U}$ be the unitary stabilizer circuit corresponding to $\mathcal{T}$. Therefore, $\mathcal{U}|0\rangle^{\otimes n} = |\psi\rangle$. The proof of converse direction is clear. □

Corollary 5. *Any n-qubit stabilizer state $|\psi\rangle$ can be transformed into the state $|0\rangle^{\otimes n}$ by applying a stabilizer circuit.*

Proof. According to Corollary 4, there is a unitary stabilizer circuit $\mathcal{U}$ such that $\mathcal{U}|0\rangle^{\otimes n} = |\psi\rangle$. It suffices to reverse $\mathcal{U}$ to do the inverse transformation. In this way, we reverse the order of gates and replace every $\boldsymbol{P}$ gate with $\boldsymbol{PPP}$. □

There is a simulation algorithm based on applying tableaus which takes $O(n^2)$ time for measurements [16]. Furthermore, tableau representation has a key role in the development of simulation algorithms in the generalized stabilizer formalism [31].

6.4 Frame representation

Let $\mathfrak{M}$ be the stabilizer matrix of an n-qubit stabilizer state $|\psi\rangle$. By modifying the leading phases $\pm$ of $\mathfrak{M}$, we can construct 2^n-1 additional orthogonal stabilizer states. These states, together with $|\psi\rangle$, form an orthonormal basis. This basis is specified by $|\psi\rangle$, and any of the other basis states specifies the same basis.

A set of $k \le 2^n$ stabilizer states $\{|\psi_j\rangle\}_{j=1}^k$ which form an orthonormal basis for a subspace of $H^{\otimes n}$, is called an n-qubit *frame* $\mathcal{F}$ [32]. We represent $\mathcal{F}$ by a pair $(\mathfrak{M}, \{\varrho_j\}_{j=1}^k)$, where $\mathfrak{M}$ is a stabilizer matrix and $\{\varrho_j\}_{j=1}^k$ is a set of distinct phase vectors with $\varrho_j \in \{+1,-1\}^n$. We represent $|\psi_j\rangle$ by $\mathfrak{M}^{\varrho_j}$ denoting the ordered assignment of the elements in ϱ_j as the ±1-phases of the rows in $\mathfrak{M}$. The *size* of the frame is denoted by $|\mathcal{F}|$, which is equal to k. As an example, for stabilizer states $|\psi_1\rangle = \frac{|00\rangle+|01\rangle}{\sqrt{2}}$ and $|\psi_2\rangle = \frac{|10\rangle+|11\rangle}{\sqrt{2}}$, with $\varrho_1 : (+,+)$ and $\varrho_2 : (-,+)$ we have

$$\mathfrak{M}^{\varrho_1} = \begin{matrix} + \\ + \end{matrix}\begin{pmatrix} Z & I \\ I & X \end{pmatrix} \equiv |\psi_1\rangle,$$

$$\mathfrak{M}^{\varrho_2} = \begin{matrix} - \\ + \end{matrix}\begin{pmatrix} Z & I \\ I & X \end{pmatrix} \equiv |\psi_2\rangle.$$

Consider state $|1\rangle$ which is stabilized by $-Z$. Conjugating the stabilizer by the phase gate gives $\boldsymbol{P}(-Z)\boldsymbol{P}^\dagger = -Z$. However, in the vector representation we have $\boldsymbol{P}|1\rangle = \mathrm{i}|1\rangle$. Hence, the global phase i is not maintained by the stabilizer. This example shows that when simulating single stabilizer states, global phases are unobservable. However, when simulating stabilizer-state superpositions, global phases become relative. To see this, we note that acting a Clifford gate u on $\mathcal{F}$ maps the basis $\{|\psi_j\rangle\}$ to $\{\mathrm{e}^{\mathrm{i}\theta_j}|\phi_j\rangle\}$, where $\mathrm{e}^{\mathrm{i}\theta_j}$ is the global phase of the stabilizer state $|\phi_j\rangle$. In other words, this operation rotates $\mathcal{F}$ and along this rotation, the superposition $|\Psi\rangle = \sum_{j=1}^k \nu_j|\psi_j\rangle$ maps to $|\Phi\rangle = \sum_{j=1}^k \nu_j \mathrm{e}^{\mathrm{i}\theta_j}|\phi_j\rangle$. Here, the global phase $\mathrm{e}^{\mathrm{i}\theta_j}$ of each $|\phi_j\rangle$ becomes relative with respect to $|\Phi\rangle$, thus we need to compute such phases.

Stabilizer frames provide a simulation algorithm based on the global-phase maintenance as follows. According to Corollary 4, for any stabilizer state $|\psi\rangle$ there exists a stabilizer circuit $\mathcal{U}$ such that $|\psi\rangle = \mathcal{U}|0\rangle^{\otimes n}$. To compute the global phase of $|\psi\rangle$, we can keep an account of the global factors generated when each gate in $\mathcal{U}$ is simulated sequentially. In this way, the global phase of each state in $\mathcal{F}$ is maintained by using the amplitude vector $\mathbf{v} = (\nu_1, ..., \nu_k) \in \mathbb{C}^k$. Each ν_j forms a pair with phase vector ϱ_j, and in the process of simulating Clifford gates u, ν_j is updated according to the following algorithm.

Algorithm 2. (Updating global phases)

1) Set the $\pm$-phases of $\mathfrak{M}$ to ϱ_j.

2) Store nonzero amplitude α of the basis state $|\tau\rangle \equiv \mathfrak{M}^{\varrho_j}$.

3) Find state $|\tau'\rangle$ and amplitude α' by computing $u(\alpha|\tau\rangle) = \alpha'|\tau'\rangle$.

4) Find $|\tau'\rangle$ by computing $u\mathfrak{M}u^\dagger$ and store its amplitude $\beta \neq 0$.

5) Update the global factor as $\nu_j \leftarrow \frac{\nu_j\,\alpha'}{\beta}$.

We note that in step 2, for $u = \boldsymbol{H}$, it may be necessary to sample a sum of two nonzero (real and imaginary) basis amplitudes.

In order to sample the computational-basis amplitudes α and α', $\mathfrak{M}$ needs to be in row-echelon form (see Theorem 9). Therefore, simulating with global phase-maintenance takes $O(kn^3)$ time. We can improve this runtime by noting that during simulation, the form of $\mathfrak{M}$ is invariant, i.e., $\mathfrak{M}$ remains in row-echelon form. This invariance can be repaired with $O(n)$ row multiplications, each of which with $\Theta(n)$ runtime. It results that updating $\mathfrak{M}$ takes $O(n^2)$ time. Hence, the overall runtime for simulating a Clifford gate is $O(n^2 + kn)$.

In the next section, we study some important classes of quantum channels, which have a key role in quantum information theory.

7 Quantum channels

Let $\Phi : \mathbb{C}^{n\times n} \to \mathbb{C}^{l\times l}$ be a linear map. Φ is called *positive*, if for any positive semi-definite matrix $A \in \mathbb{C}^{n\times n}$, $\Phi(A) \in \mathbb{C}^{l\times l}$ is so. Given a positive integer m, Φ is called *m-positive*, if $\Phi \otimes \mathrm{Id}_m : \mathbb{C}^{n\times n} \bigotimes \mathbb{C}^{m\times m} \to \mathbb{C}^{l\times l} \bigotimes \mathbb{C}^{m\times m}$ is a positive map, where $\mathrm{Id}_m : \mathbb{C}^{m\times m} \to \mathbb{C}^{m\times m}$ is the identity map. Φ is called *completely positive*, if for any positive integer m, Φ is m-positive. Φ is called *trace-preserving*, if $\mathrm{tr}(\Phi(A)) = \mathrm{tr}(A)$, for every A. A completely positive and trace-preserving map is called *quantum channel*. For example, *Pauli channel* Φ_P maps an input state with density operator ρ as follows:

$$\Phi_P(\rho) = p_0 I\rho I + p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z,$$

where $p_i \geq 0$ and $\sum_i p_i = 1$. In the case of $p_x = p_y = p_z = \frac{p}{3}$, the Pauli channel is called the *depolarizing channel*, which is one of the most important instances of diagonal channels [33].

7.1 Stabilizer channels

A quantum channel Φ that maps any stabilizer state $|\psi\rangle\langle\psi|$ to a stabilizer state $\Phi(|\psi\rangle\langle\psi|)$ is called a *stabilizer channel*. Stabilizer channels include two classes of quantum channels. The first one is the class of Clifford channels, i. e. channels that map ρ to $u\rho u^\dagger$ where u is a Clifford operator. The second one is the class of nonunitary channels on the space of stabilizer states, which map any state to a determined state.

A *Pauli reset channel* associated with a Pauli product u is an example of stabilizer channels, which sets any given qubit to a $+1$ eigenvector of u. This channel is denoted by R_u and can be written as follows:

$$R_u(\rho) = \frac{I+u}{2}\rho\frac{I+u}{2} + \boldsymbol{C}_{u\to -u}\frac{I-u}{2}\rho\frac{I-u}{2}, \qquad (16)$$

where $\boldsymbol{C}_{u\to -u}$ is the Clifford channel that maps u to $-u$. We note that $\frac{I\pm u}{2}$ is the projector onto the ± 1 eigenspace of u. Stabilizer channels give rise to calculate the expectation value for an observable on the final state of a circuit by using the Monte Carlo method [34].

Theorem 11. *Any quantum channel Φ can be decomposed as $\Phi = \sum_i \lambda_i \Psi_i$, where Ψ_i's are stabilizer channels and $\lambda_i \in \mathbb{R}$ with $\sum_i \lambda_i = 1$.*

Proof. For Pauli products u and u', let $\Phi_{u\to u'}$ be the superoperator (generally unphysical channel) that maps u to u' and every other Pauli product to 0. Since Pauli products span the space of operators on n qubits, thus $\{\Phi_{u\to u'}\}$ is a basis for the space of n qubit channels. For Pauli products u and v we define $\triangle(u,v) := 1(-1)$ when u and v commute (anti-commute). Since every nonidentity Pauli product u commutes with exactly half of the Pauli products and anti-commutes with the remaining elements, then

$$\sum_v \triangle(u,v) = \begin{cases} 4^n & \mathrm{u} = I, \\ 0 & \text{otherwise.} \end{cases} \qquad (17)$$

Let Φ_v be the channel that maps ρ to $v\rho v^\dagger$, then by applying Eq. (17) and the fact that $\triangle(u,v)\triangle(u',v) = \triangle(uu',v)$ we have

$$\begin{aligned} \sum_v \triangle(u,v)\Phi_v(u') &= \sum_v \triangle(u,v) v u' v^\dagger \\ &= u' \sum_v \triangle(u,v)\triangle(u',v) \\ &= \begin{cases} 4^n u' & u' = u, \\ 0 & \text{otherwise} \end{cases} = 4^n \Phi_{u\to u}(u'). \end{aligned} \qquad (18)$$

It shows that $\Phi_{u\to u}$ can be decomposed as a linear combination of stabilizer channels with real coefficients summing to 1. By applying Eq. (16) we obtain the following decomposition for $\Phi_{I\to u}$ where $u \neq I$,

$$\Phi_{I\to u} = R_u\Phi_{I\to I} - \Phi_{I\to I}. \qquad (19)$$

For $u \neq u'$ and $u, u' \neq I$, we can decompose $\Phi_{u\to u'}$ as follows

$$\Phi_{u\to u'} = \boldsymbol{C}_{u\to u'}\Phi_{u\to u}, \qquad (20)$$

where $\boldsymbol{C}_{u\to u'}$ is the Clifford channel that maps u to u'. We take into account that a quantum channel cannot have a superoperator of the form $\Phi_{u\to I}$ as a component, since this superoperator maps two operators $\frac{I+u}{2}$ and $\frac{I-u}{2}$ which have equal traces to operators with nonequal traces. Equations (18)–(20) show that each allowed basis element $\Phi_{u\to u'}$ can be decomposed as desired, so can any quantum channel. □

This decomposition is more important than the decomposition of unitary channels as the complex linear combinations of Pauli channels [16]. In fact, the importance of this decomposition is that it can represent both unitary and non-unitary channels. As an example, let $\Psi_T : \rho \mapsto T\rho T^\dagger$, $\Psi_Z : \rho \mapsto Z\rho Z$ and $\Psi_{\boldsymbol{P}} : \rho \mapsto \boldsymbol{P}\rho\boldsymbol{P}^\dagger$ be the

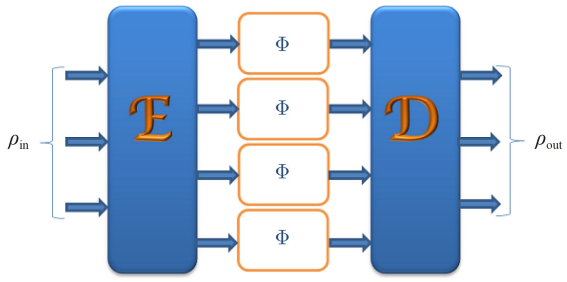


Fig. 3 Quantum information transfer using a code has a rate $\frac{k}{n}$ of $\frac{3}{4}$.

channels corresponding to $T := \sqrt{\boldsymbol{P}}$, Z and $\boldsymbol{P}$ gates, respectively. We have the following stabilizer decomposition

$$\Psi_T = \frac{1}{2}\boldsymbol{I} + \frac{1-\sqrt{2}}{2}\Psi_Z + \frac{\sqrt{2}}{2}\Psi_{\boldsymbol{P}},$$

where $\boldsymbol{I}$ is the identity channel.

We note that the stabilizer decomposition is not unique and λ_i's may be negative. Each term in this decomposition describes a physical process and only when $\lambda_i \geq 0$ for all i, they can be interpreted as probabilities of physical processes. Generally, λ_i's may be considered as a quasiprobability distribution. Accordingly, we can define *negativity* of a decomposition as follows: $\varsigma = \sum_{i:\lambda_i<0} |\lambda_i|$. In fact, $\varsigma > 0$ indicates nonclassical behaviour and traces back to the development of the Wigner function [35].

7.2 Capacity of the erasure channel

The capacity of a quantum channel is the highest rate of reliable information transmission through many independent uses of the channel. To determine reliability, we need to compare the input and output states, ρ_{in} and ρ_{out}, by applying the following functional which is called the *fidelity*, $\boldsymbol{F} = \langle\psi|\rho_{\text{out}}|\psi\rangle$, where $\rho_{\text{in}} = |\psi\rangle\langle\psi|$ and ρ_{out} is typically a mixed state. The *quantum capacity* $\mathtt{C}_\Phi$ of a quantum channel Φ is the largest number $\mathtt{C}$ such that for any $\mathtt{R} < \mathtt{C}$ and any $\epsilon > 0$, there are block sizes k and n and a quantum error-correcting code mapping states $|\psi\rangle$ of k qubits into n independent uses of the channel with $\frac{k}{n} > \mathtt{R}$, such that every state $|\psi\rangle$ can be recovered with fidelity at least $1-\epsilon$ at the receiving end.

The encoder $\mathcal{E}$ and decoder $\mathcal{D}$ are completely positive and trace preserving maps such that $\mathcal{E}$ maps k qubits into n intermediate systems, then each of them is sent through an independent instance of the channel Φ, and finally $\mathcal{D}$ maps the n channel outputs into k qubits (Fig. 3).

A *quantum erasure channel* with probability p is a quantum channel from states in $H \simeq \mathbb{C}^2$ into states in $H \oplus \mathbb{C}|2\rangle \simeq \mathbb{C}^3$ defined by

$$\Phi_p : |\psi\rangle\langle\psi| \longmapsto (1-p)|\psi\rangle\langle\psi| + p|2\rangle\langle 2|,$$

where $|2\rangle$ is an orthogonal state to H and corresponds to a lost qubit. When we apply the erasure channel, each qubit is erased independently with probability p. An erased qubit is subjected to a random uniform Pauli error (I, X, Y or Z with equal probability $\frac{1}{4}$) and we know that this qubit is erased.

For n qubits, the *characteristic vector* of the erased locations, $\mathcal{E}^p = ((\mathcal{E}^p)_1, ..., (\mathcal{E}^p)_n)$, is defined as an element of $\mathbb{F}_2^n$ which each of its components follows a Bernoulli distribution of probability p. When a quantum state is subjected to a random Pauli error $E = E_1...E_n \in \mathcal{P}_n$, the qubit in location i is lost if and only if $(\mathcal{E}^p)_i = 1$. And $E_i = I$ if $(\mathcal{E}^p)_i = 0$. We say that erasure $\mathcal{E}^p$ *covers* the error E, if $\mathtt{Supp}(E) \subset \mathcal{E}^p$, i.e., the support of E is included in the set of erased locations.

An encoded state $|\psi\rangle$ is transformed by a random error E into a state $E|\psi\rangle$ for which we know that $\mathcal{E}^p$ covers E. To recover the original state, we need to compute the corresponding syndrome of E and then infer an error E' covered by $\mathcal{E}^p$. If E and E' are in the same coset of $\mathcal{P}_n/S$, then $E'E|\psi\rangle = |\psi\rangle$ and therefore the effect of E is corrected. In this case, the erasure is called *correctable*. If E' is not equivalent to E, we cannot recover the quantum state in general. In this case, the erasure is called *non-correctable*. To see an example of a non-correctable erasure, refer to Ref. [36].

The capacity of Φ_p is upper bounded by $1-2p$, which follows from the no-cloning theorem, see Ref. [37]. Hence, it does not rely on the quantum code structure. Therefore, we can find achievable rates of stabilizer codes over Φ_p and then the capacity is derived. A family of quantum codes $\mathcal{Q} = \{Q_n\}_{n=1}^{\infty}$ is called *capacity achieving* if for sufficiently large n, we can find a code $Q_n \in \mathcal{Q}$ with rate arbitrarily close to the capacity. Theorem 12 shows that the family of stabilizer codes is capacity achieving over Φ_p, thus $\mathtt{C}_{\Phi_p} = 1-2p$.

Theorem 12. ([36]) *Let $\mathcal{Q}$ be a family of stabilizer codes of rates $\mathfrak{R}$ and achieving vanishing decoding error probability over Φ_p. Furthermore, suppose that every code $Q \in \mathcal{Q}$ has a set of generators of its stabilizer whose weights are upper bounded by m. Then*

$$\mathfrak{R} \leq (1-2p)\frac{1-(1-p)^{m-1}}{1-(1-2p)(1-p)^{m-1}}.$$

Compared to Pauli errors, erasures or errors with known locations are a more desirable error type for quantum error-correcting codes. Therefore, transforming physical noise into erasures can considerably improve the performance of quantum error correction [38].

8 Tomography

The main task of tomography is to reconstruct a full classical description of an n-qubit state from experimental

data. In the process of developing methods of tomography, the following question entitled *shadow tomography problem* is raised. Given an n-qubit state ρ and two-outcome measurements $\mathcal{M}_1, \mathcal{M}_2, ..., \mathcal{M}_m$, estimate $\mathrm{tr}[\mathcal{M}_i\rho]$ up to error ϵ, for $i = 1, 2, ..., m$. This problem is solved by designing a quantum procedure with $\widetilde{O}(\epsilon^{-4} \cdot \log^4 m \cdot \log n)$ copies of state, where $\widetilde{O}$ hides factors which are polynomial in $\log\log m, \log\log n$ and $\log\epsilon^{-1}$ [39].

After this brief introductory note, let us describe the framework of classical shadows. Let ρ be an unknown n-qubit state. First we apply a set of unitary evolutions $\rho \mapsto u\rho u^\dagger$, where u is randomly selected from an ensemble $\mathfrak{U}$ and then we measure the rotated state in the computational basis $\{|b\rangle : b \in \{0,1\}^n\}$. Here, different ensembles lead to different versions of procedure and in practical scheme, each ensemble unitary should be realizable as an efficient quantum circuit. We suppose that this collection is tomographically complete, i.e., for each $\tau \neq \rho$ there are $u \in \mathfrak{U}$ and b such that $\langle b|u\tau u^\dagger|b\rangle \neq \langle b|u\rho u^\dagger|b\rangle$. The framework of classical shadow estimation is based on the following algorithm.

Algorithm 3. (Constructing classical shadow)

1) Prepare a copy of the unknown quantum state ρ.

2) Sample $u \sim \mathfrak{U}$ randomly.

3) Transform $u \mapsto u\rho u^\dagger$.

4) Perform a measurement in the computational basis.

5) Apply the inverse of u to the resulting state from 4 for collapsing ρ to $u^\dagger|\hat{b}\rangle\langle\hat{b}|u$, where $\mathbb{P}(\hat{b} = b) = \langle b|u\rho u^\dagger|b\rangle$.

6) Let $\mathcal{M}_{\mathfrak{U}}(\rho) := \mathbb{E}(u^\dagger|\hat{b}\rangle\langle\hat{b}|u) = \mathbb{E}_{u\sim\mathfrak{U}} \sum_{b\in\{0,1\}^n} \langle b|u\rho u^\dagger|b\rangle$ $u^\dagger|b\rangle\langle b|u$.

7) Construct a classical snapshot by computing $\hat{\rho} = \mathcal{M}_{\mathfrak{U}}^{-1}(u^\dagger|\hat{b}\rangle\langle\hat{b}|u)$.

State $\hat{\rho}$ is called *classical shadow*, which has a unit trace, but need not be positive semi-definite. We note that tomographically completeness ensures that $\mathcal{M}_{\mathfrak{U}}^{-1}$ exists.

Classical shadow is a useful tool in numerical experiments based on random Clifford measurements [40]. We know that a stabilizer circuit can be simulated efficiently in $O(n^2)$ time by applying the algorithm based on tableau representation. This algorithm enables us to simulate systems efficiently with even more than 160 qubits in practice. To test the performance of predicting with classical shadows, we need to implement repeatedly the following efficient protocol.

1) Sample a Clifford unitary u from $\mathcal{C}_n$ by applying the algorithm proposed in Ref. [41].

2) The action of u on X- and Z-type operators is fully characterized by parameters

$(\alpha, \beta, \gamma, \delta, r, t)$ as follows:

$$uX_j u^\dagger = (-1)^{r_j} \prod_{i=1}^{n} X_i^{\alpha_{ji}} Z_i^{\beta_{ji}},$$

$$uZ_j u^\dagger = (-1)^{t_j} \prod_{i=1}^{n} X_i^{\gamma_{ji}} Z_i^{\delta_{ji}},$$

where $j = 1, 2, ..., n$ and $r_j, t_j, \alpha_{ji}, \beta_{ji}, \gamma_{ji}$ and $\delta_{ji} \in \{0, 1\}$.

3) A parameterized unitary u by $(\alpha, \beta, \gamma, \delta, r, t)$ can be applied on stabilizer states by changing the stabilizer generators and the destabilizer generators.

4) A computational basis measurement can be simulated by the improved algorithm based on tableau representation.

9 Discussion

In this section, we present some research lines as follows.

- The family of quantum low-density parity-check (qLDPC) codes is a subclass of CSS codes, which plays a central role in classical error correction [43]. Existence of qLDPC codes whose minimal distance scales linearly with the number of qubits is one of the major open problems in quantum information [44]. Furthermore, to see a set of open problems on geometric and combinatorial aspects of qLDPC codes, refer to Ref. [45].
- The XP stabilizer formalism is an extension of the stabilizer formalism which includes fractional $\frac{2\pi}{n}$ rotations around the Z axis, where n is an integer. There is an equivalence between XP stabilizer states and weighted hypergraph states. To see a set of open problems in the XP stabilizer formalism, refer to Ref. [46].

10 Conclusion

The process of measuring a Pauli observable is discussed. It is shown that there exists a stabilizer witness consisting of a full set of generators, which is coarser than the GHZ witness. Moreover, with less than n generators, it is not possible to detect genuine n-qubit entanglement. A stabilizer code is constructed from a given linear code. The evolution of a quantum system in the presence of noise is discussed by giving the error-correcting criteria. Moreover, the process of syndrome extraction for correctable errors is discussed. By applying logical bases, it is shown that any stabilizer code is unitarily equivalent to a trivial code. Given a graph code, its stabilizer generators are obtained. By applying the cleaning lemma, the distance of a stabilizer code embeddable in a lattice is given. By applying stabilizer matrices, the runtime of simulating stabilizer gates is obtained. The Knill–Gottesman theorem on classical simulation of stabilizer circuits is discussed. It is shown that given a full tableau, every Pauli product can be decomposed efficiently into a product of a stabilizer and a destabilizer. An algorithm for updating global phases by applying frame representation is given. Resolution of a quantum channel into a sum of stabilizer channels is shown. A family of capacity achieving stabilizer codes is applied to obtain the capacity of the quantum erasure channel. An algorithm for constructing classical shadow is given.

Acknowledgements This work was performed in the Laboratory of Combinatorial and Geometric Structures, School of Applied Mathematics and Informatics, MIPT. I would like to thank Prof. Andrei M. Raigorodskii, Dr. Andrey B. Kupavskii and my colleagues.

References

1. D. Gottesman, Stabilizer codes and quantum error correction, arXiv: quant-ph/9705052, Caltech Ph.D thesis, 1997
2. K. Fujii, Stabilizer formalism and its applications, in: Quantum Computation with Topological Codes, Springer Briefs in Mathematical Physics, Vol. 8, Singapore: Springer, 2015
3. D. Gottesman, The Heisenberg representation of quantum computers, arXiv: quant-ph/9807006 (1998)
4. F. R. F. Pereira, S. Mancini, and G. G. La Guardia, Stabilizer codes for open quantum systems, *Sci. Rep.* 13(1), 10540 (2023)
5. A. Dymarsky and A. Shapere, Quantum stabilizer codes, lattices, and CFTs, *J. High Energy Phys.* 2021(3), 160 (2021)
6. D. Schlingemann and R. F. Werner, Quantum error-correcting codes associated with graphs, *Phys. Rev. A* 65(1), 012308 (2001)
7. A. Dahlberg and S. Wehner, Transforming graph states using single-qubit operations, *Philos. Trans. Royal Soc. A* 376(2123), 20170325 (2018)
8. D. Markham and B. C. Sanders, Graph states for quantum secret sharing, *Phys. Rev. A* 78(4), 042309 (2008)
9. J. Ribeiro, G. Murta, and S. Wehner, Fully device-independent conference key agreement, *Phys. Rev. A* 97(2), 022307 (2018)
10. M. Christandl and S. Wehner, Quantum anonymous transmissions, in: Advances in Cryptology – ASIACRYPT (Ed. R. Bimal), pp 217–235, Berlin: Springer, 2005
11. R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, Quantum clock synchronization based on shared prior entanglement, *Phys. Rev. Lett.* 85(9), 2010 (2000)
12. V. Veitch, S. A. Hamed Mousavian, D. Gottesman, and J. Emerson, The resource theory of stabilizer quantum computation, *New J. Phys.* 16(1), 013009 (2014)
13. C. H. Bennett and S. J. Wiesner, Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states, *Phys. Rev. Lett.* 69(20), 2881 (1992)
14. D. M. Greenberger, M. A. Horne, and A. Zeilinger, Bell' s Theorem, Quantum Theory, and Conceptions of the Universe, Kluwer, 1989
15. C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels, *Phys. Rev. Lett.* 70(13), 1895 (1993)
16. S. Aaronson and D. Gottesman, Improved simulation of stabilizer circuits, *Phys. Rev. A* 70(5), 052328 (2004)
17. P. Selinger, Generators and relations for n-qubit Clifford operators, *Log. Methods Comput. Sci.* 11(2), 1 (2015)
18. M. Horodecki, P. Horodecki, and R. Horodecki, Asymptotic manipulations of entanglement can exhibit genuine irreversibility, *Phys. Rev. Lett.* 86(25), 5844 (2001)
19. C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe, Experimental entanglement of four particles, *Nature* 404(6775), 256 (2000)
20. G. Tóth and O. Gühne, Entanglement detection in the stabilizer formalism, *Phys. Rev. A* 72(2), 022340 (2005)
21. D. Dieks, Communication by EPR devices, *Phys. Lett. A* 92(6), 271 (1982)
22. E. Knill, R. Laflamme, and L. Viola, A theory of quantum error correcting codes, *Phys. Rev. Lett.* 84(11), 2525 (2000)
23. J. Preskill, Lecture Notes for Physics 229: Quantum Information and Computation, Create Space Independent Publishing Platform, 2015
24. M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, Entanglement in graph states and its applications, arXiv: quant-ph/0602096 (2006)
25. D. Schlingemann, Stabilizer codes can be realized as graph codes, *Quantum Inf. Comput.* 2(4), 307 (2002)
26. T. J. Bell, L. A. Pettersson, and S. Paesani, Optimizing graph codes for measurement-based loss tolerance, *PRX Quantum* 4(2), 020328 (2023)
27. J. Haah and J. Preskill, Logical operator tradeoff for local quantum codes, *Phys. Rev. A* 86(3), 032308 (2012)
28. S. Bravyi and B. Terhal, A no–go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes, *New J. Phys.* 11(4), 043029 (2009)
29. A. R. Arab, On states of quantum theory, *Int. J. Geom. Methods Mod. Phys.* 19(14), 2250221 (2022)
30. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, 10th Anniversary Edition, Cambridge University Press, 2010
31. T. J. Yoder, A generalization of the stabilizer formalism for simulating arbitrary quantum circuits, www.scottaaronson.com/showcase2/report/ted-yoder.pdf (2012)
32. H. J. García and I. L. Markov, Simulation of quantum circuits via stabilizer frames, *IEEE Trans. Comput.* 64(8), 2323 (2015)
33. A. R. Arab, On diagonal quantum channels, *Rep. Math. Phys.* 88(1), 59 (2021)
34. R. S. Bennink, E. M. Ferragut, T. S. Humble, J. A. Laska, J. J. Nutaro, M. G. Pleszkoch, and R. C. Pooser, Unbiased simulation of near-Clifford quantum circuits, *Phys. Rev. A* 95(6), 062337 (2017)
35. E. Wigner, On the quantum correction for thermodynamic equilibrium, *Phys. Rev.* 40(5), 749 (1932)
36. N. Delfosse and G. Zémor, Upper bounds on the rate of low density stabilizer codes for the quantum erasure channel, *Quantum Inf. Comput.* 13(9–10), 793 (2013)
37. C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, Capacities of quantum erasure channels, *Phys. Rev. Lett.* 78, 3217 (1997)
38. M. Kang, W. C. Campbell, and K. R. Brown, Quantum error correction with metastable states of trapped ions using erasure conversion, *PRX Quantum* 4(2), 020358

(2023)
39. S. Aaronson, Shadow tomography of quantum states, arXiv: 1711.01053 (2017)
40. H. Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, *Nat. Phys.* 16(10), 1050 (2020)
41. R. Koenig and J. A. Smolin, How to efficiently select an arbitrary Clifford group element, *J. Math. Phys.* 55(12), 122202 (2014)
42. A. M. Steane, A Tutorial on Quantum Error Correction, Quantum Computers, Algorithms and Chaos, pp 1–32, Amsterdam: IOS Press, 2006
43. R. G. Gallager, Low-density parity-check codes, *IRE Trans. Inf. Theory* 8(1), 21 (1962)
44. L. Eldar, M. Ozols, and K. Thompson, The need for structure in quantum LDPC codes, *IEEE Trans. Inf. Theory* 66(3), 1460 (2020)
45. N. P. Breuckmann and J. N. Eberhardt, Quantum low-density parity-check codes, *PRX Quantum* 2(4), 040101 (2021)
46. M. A. Webster, B. J. Brown, and S. D. Bartlett, The XP stabiliser formalism: A generalisation of the Pauli stabiliser formalism with arbitrary phases, *Quantum* 6, 815 (2022)
47. A. L. Grimsmo and S. Puri, Quantum error correction with the Gottesman–Kitaev–Preskill code, *PRX Quantum* 2(2), 020101 (2021)